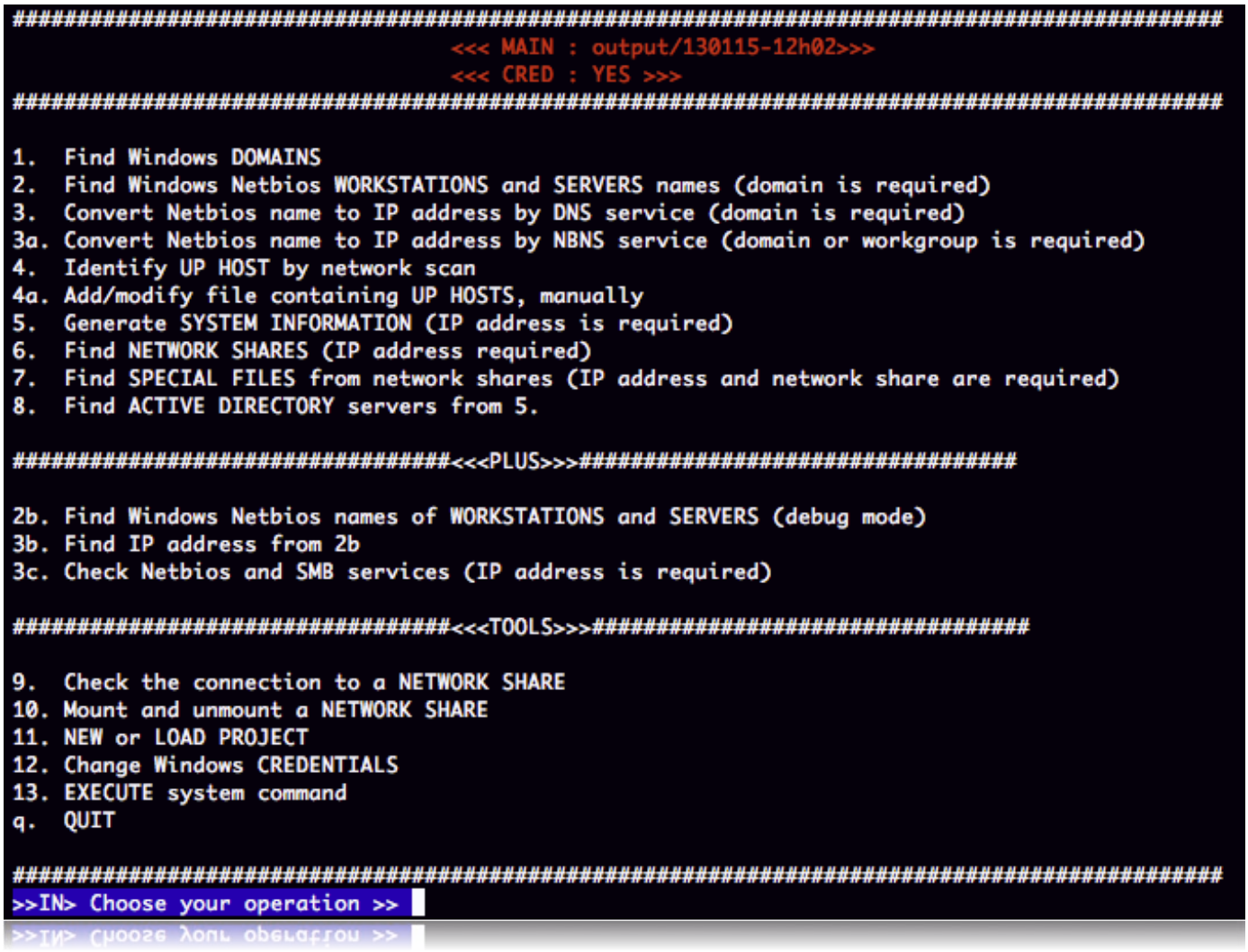
Net2SharePwn

Readme

R E A D M E



Net2SharePwn

Readme

CONTENTS

Net2SharePwn

Readme

Usage of Net2SharePwn

Net2SharePwn is an utility to check and exploit automatically the NetBIOS Network Shares available from network access points.
Question: How do you identify THE FILE containing a password to elevate your network or system privileges, when too much domains or IP addresses are present? The time is an important factor in this situation … and during penetration testing, it's common to identify a VBS script embedding a domain administrator account password.
Answer: *Net2SharePwn* has been built to allow that.

Net2SharePwn is built in **Python** (tested on Python2.6) and can be launched only on **Linux (tested on Backtrack) and Mac OS x platforms**.

I apologize for Python coding, it doesn't respect the best practices but I didn't predict to publish *Net2SharePwn* …
Net2SharePwn is perhaps developed "with my feet" but it is functional.

You can, if you want to, modify this program to adapt it for your personal usage.

System dependencies

Net2SharePwn uses several system commands like:

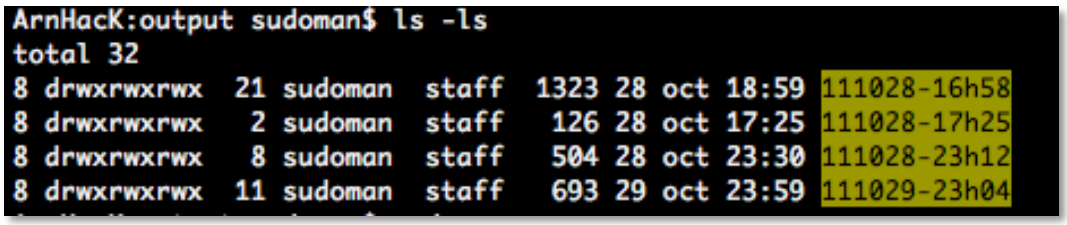
- smbtree
- smbclient
- nmap
- arp-scan (to install for Backtrack)
- nmblookup
- mount_smbfs

Before usage, please check if these packages are installed on your system.

Moreover, due to dependencies, it is necessary to launch Net2SharePwn with **root privileges**.

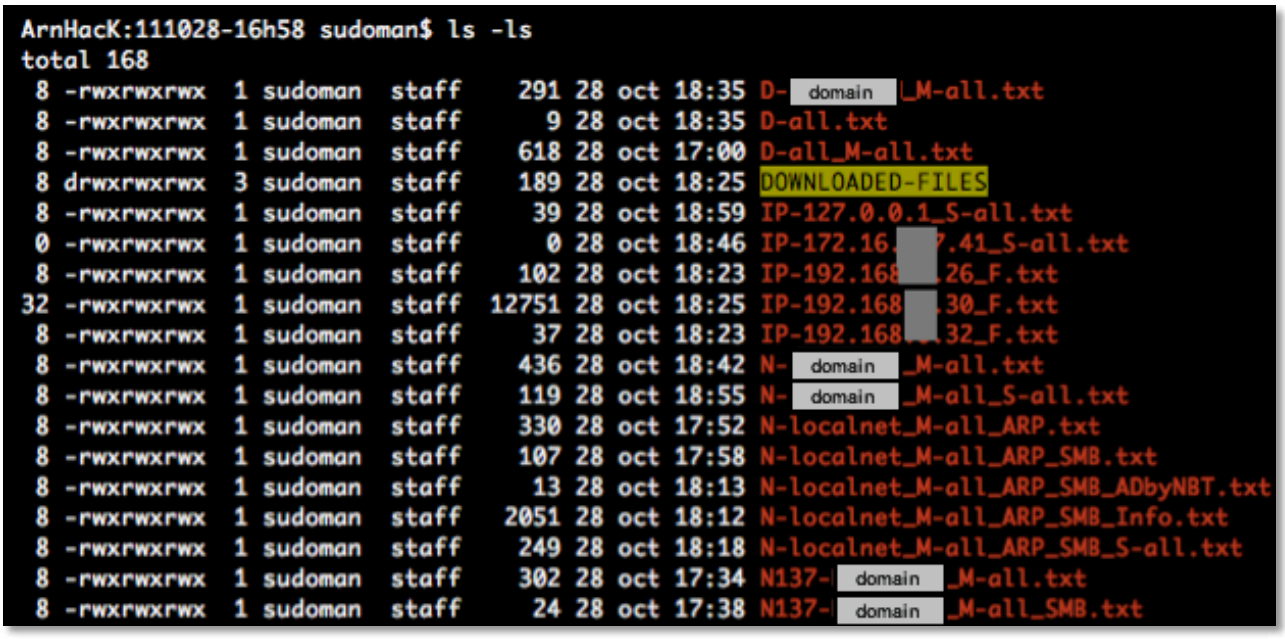
Projects management

For *Net2SharePwn*, a project is a folder stored in the "output" directory. It stores the results of all launched tests.
Net2SharePwn allows creating a new project or load an existing project.



Net2SharePwn

Readme



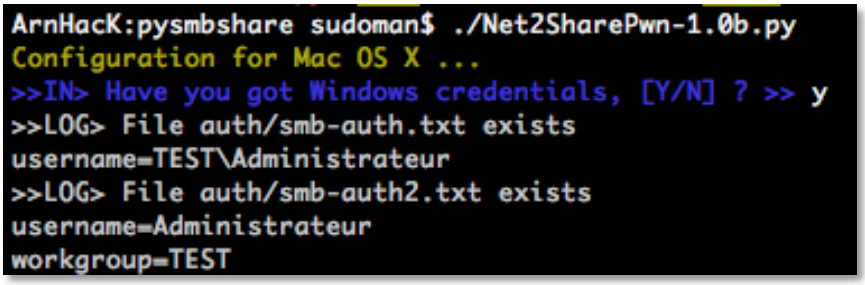
See “Net2SharePwn starting” and “NEW or LOAD PROJECT” sections for more details.

Windows authentication

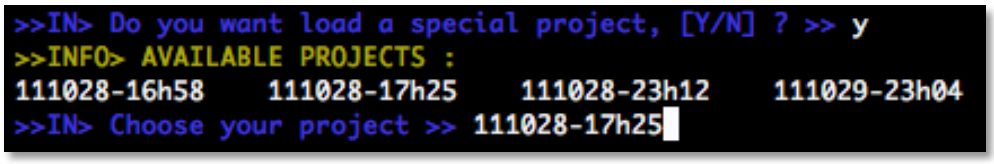
Net2SharePwn allows launching all the tests with or without a Windows domain account.
See “Net2SharePwn starting” and “Change Windows CREDENTIALS” sections for more details.

Net2SharePwn starting

When you launch *Net2SharePwn*, the first step is to choose if you have Windows credentials or not.



If you have Windows credentials, the files “auth/smb-auth.txt” and “auth/smb-auth2.txt” are used.
Don’t directly modify these files, there is a special function for that. See “Change Windows CREDENTIALS” for more details.
The second step is to load or not an existing project storing previous results.



Net2SharePwn

Readme

If you want to load a previous project, you have to choose the directory name.

After that, you can use Net2SharePwn.

```
>>IN> Choose your project >> 130109-06h22
#############################################################################################
                                <<< MAIN : output/130109-06h22>>>
                                <<< CRED : YES >>>
#############################################################################################

1.  Find Windows DOMAINS
2.  Find Windows Netbios WORKSTATIONS and SERVERS names (domain is required)
3.  Convert Netbios name to IP address by DNS service (domain is required)
3a. Convert Netbios name to IP address by NBNS service (domain or workgroup is required)
4.  Identify UP HOST by network scan
4a. Add/modify file containing UP HOSTS, manually
5.  Generate SYSTEM INFORMATION (IP address is required)
6.  Find NETWORK SHARES (IP address required)
7.  Find SPECIAL FILES from network shares (IP address and network share are required)
8.  Find ACTIVE DIRECTORY servers from 5.

##################################<<<PLUS>>>#################################

2b. Find Windows Netbios names of WORKSTATIONS and SERVERS (debug mode)
3b. Find IP address from 2b
3c. Check Netbios and SMB services (IP address is required)

#################################<<<TOOLS>>>#################################

9.  Check the connection to a NETWORK SHARE
10. Mount and unmount a NETWORK SHARE
11. NEW or LOAD PROJECT
12. Change Windows CREDENTIALS
13. EXECUTE system command
q.  QUIT

#############################################################################################
>>IN> Choose your operation >>
```

For information, the main menu indicates the project name and if you have got or not Windows credentials.

```
#####################################
 <<< MAIN : output/130109-06h22>>>
 <<< CRED : YES >>>
#####################################
```

```
#####################################
 <<< MAIN : output/130115-12h24>>>
 <<< CRED : NO >>>
#####################################
```

Net2SharePwn

Readme

Main functions

a. Find Windows DOMAINS

Objective >This function allows to identify Windows Domains and Workgroups available from your network connection
Input >*None*
Output >`D-all.txt`

```
>>IN> Choose your operation >> 1
>>IN> Do you want to delete the previous results [Y/N] ? >> y
>>LOG> SEARCHING FOR DOMAINS, BE PATIENT ...
>RES> FOUND DOMAINS >>
WORKGROUP
TEST
>>IN> Do you want to find machines [Y/N] ? >> n
>>PRESS ANY KEY TO CONTINUE
```

b. Find Windows NetBIOS WORKSTATIONS and SERVERS names

Objective >This function allows to identify the NetBIOS workstations and servers names belonging to a special Windows domain or workgroup.
Input >`D-all.txt`
Output >`D-all_M-all.txt, D-<YourDomain>_M-all.txt`

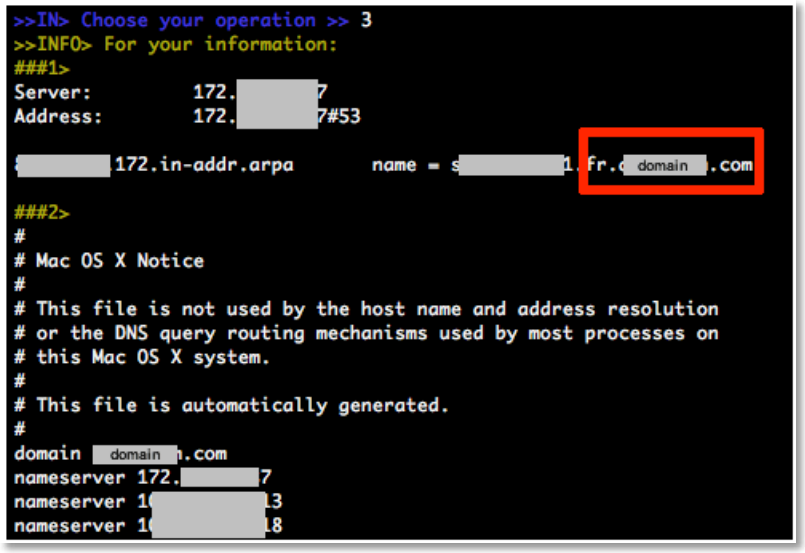
```
>>IN> Choose your operation >> 2
>>INFO> The following lists of found domains (workgroups) are available >>
WORKGROUP
TEST
>>IN> Choose a domain >> TEST
Do you want to delete the previous results [Y/N] ? >> y
Do you want to generate a new file D-all_M-all.txt [Y/N] ? >> y
>>LOG> SEARCHING FOR WINDOWS NETBIOS NAMES, BE PATIENT ...
>>RES> FOUND MACHINES FOR [TEST] DOMAIN>>
ES[redacted]A
DV[redacted]96
DV[redacted]83
DV[redacted]53
DV[redacted]79
DV[redacted]60
DV[redacted]49
DV[redacted]71
...
DV[redacted]31
DV[redacted]86
DV[redacted]79

>>INFO> RESULTS STORED IN [output/111029-23h04/D-TEST_M-all.txt]
>>PRESS ANY KEY TO CONTINUE
```

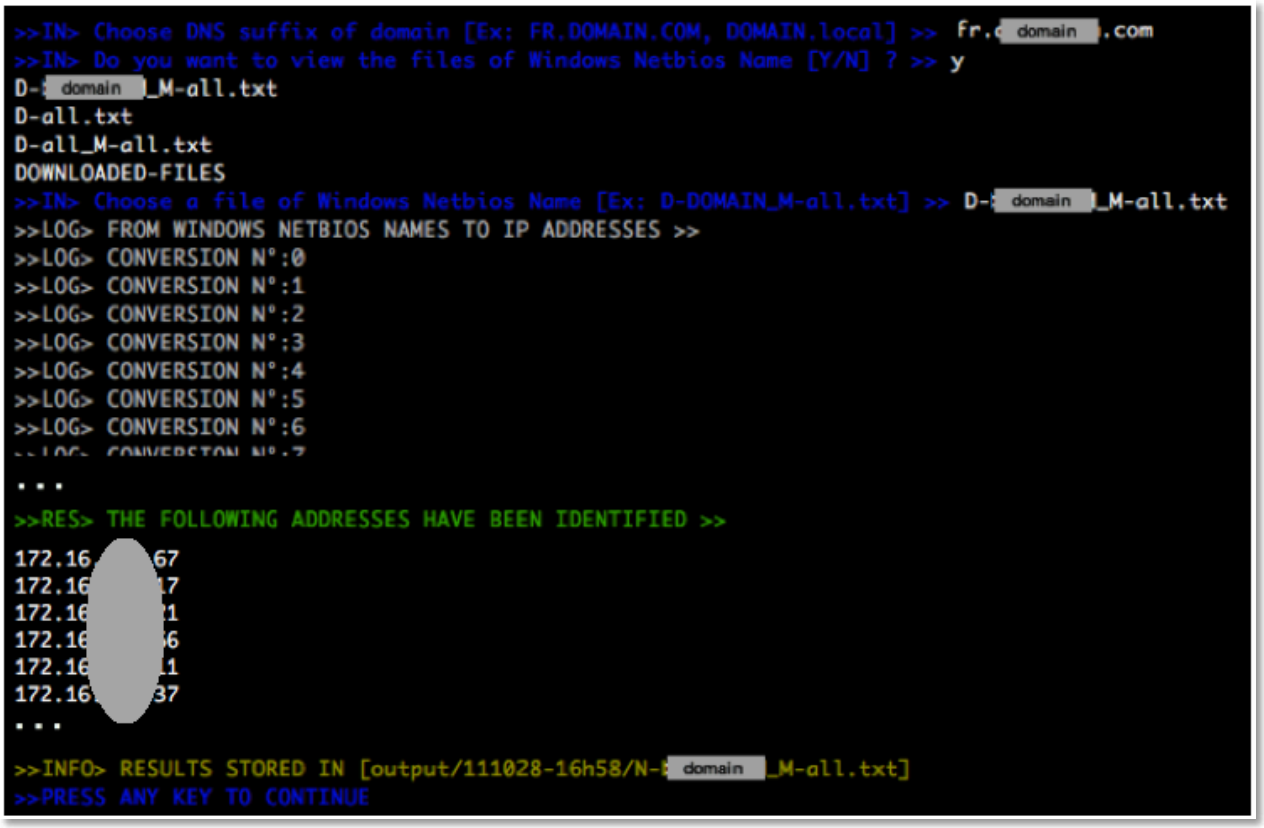
c. Convert NetBIOS name to IP address by DNS service

Objective >This function allows to convert a NetBIOS name to an IP address using DNS requests (UDP/53 on configured DNS) Input >D-<YourDomain>_M-all.txt Output >N-<YourDomain>_M-all.txt

Before launching the conversion, it is necessary to identify the DNS suffix.

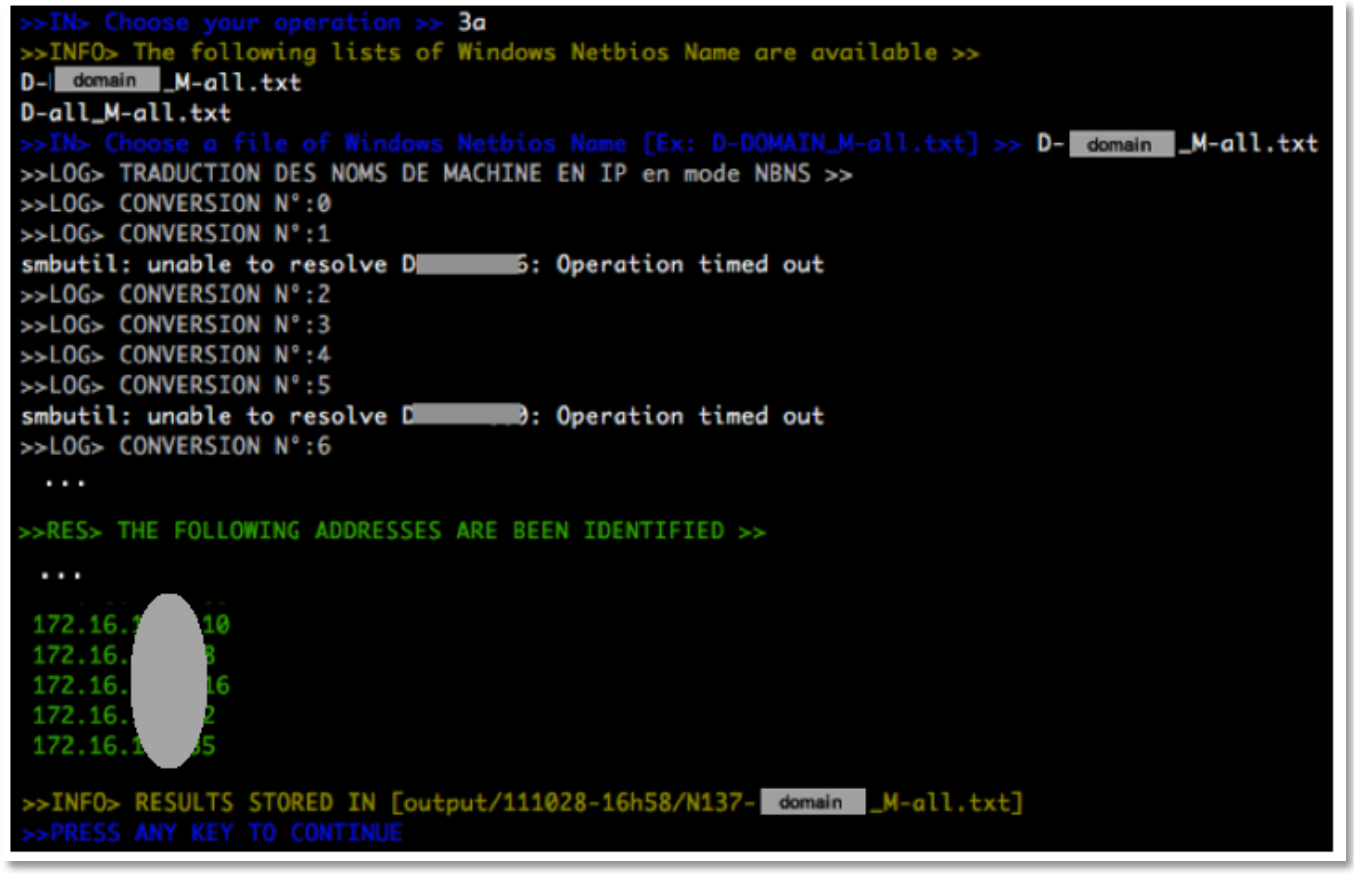


The network resolution of DNS servers allows identifying the DNS suffix.



d. Convert NetBIOS name to IP address by NBNS service

Objective >This function allows to convert a NetBIOS name to an IP address using NBNS requests (UDP/137 to IP Broadcast)
Input >`D-<YourDomain>_M-all.txt`
Output >`N137-<YourDomain>_M-all.txt`



e. Identify UP HOST by network scan

Objective >This function allows to identify IP addresses available from your network connection using 3 different ways:

1. ARP scanning
2. NBNS scanning
3. Port scanning on Netbios and SMB services

Input >None
Output >

1. after ARP scanning >`N-localnet_M-all_ARP.txt`
2. after NBNS scanning >`N-<YourIPRange_ClassC>_M-all_NBNS.txt`
3. after port scanning on Netbios and SMB services >`N-<YourSubNetwork>NET<YouMask>_M-all_SMB.txt`

Net2SharePwn

Readme

```
>>IN>Scan ARP[1], Scan NBNS[2], Scan TCP 139/445[3] >> 1
>>IN> Interface Name >> tap1
192.168.0.1     00:80:[redacted]:9a       D-LINK
192.168.0.2     00:03:[redacted]:01       Intel
192.168.0.3     00:03:[redacted]:01       Intel
192.168.0.11    00:11:[redacted]:48       ASUSTek
192.168.0.10    00:1c:[redacted]:09       Hewlett
192.168.0.20    00:0c:[redacted]:b6       VMware.
...
192.168.0.219   00:ff:[redacted]:33       (Unknown)
192.168.0.232   00:ff:[redacted]:81       (Unknown)
192.168.0.233   00:ff:[redacted]:dd       (Unknown)
192.168.0.210   00:ff:[redacted]:7b       (Unknown)
192.168.0.254   00:0a:[redacted]:2c       3COM


>>RES> THE FOLLOWING ADDRESSES HAVE BEEN IDENTIFIED >>
192.168.0.1
192.168.0.2
192.168.0.3
192.168.0.11
192.168.0.10
192.168.0.20
192.168.0.21
...
192.168.0.232
192.168.0.233
192.168.0.210
192.168.0.254

>>INFO> RESULTS STORED IN [output/111028-16h58/N-localnet_M-all_ARP.txt]
>>PRESS ANY KEY TO CONTINUE
```

```
>>IN>Scan ARP[1], Scan NBNS[2], Scan TCP 139/445[3] >> 2
>>IN> Choose the base network address [Ex: 192.168.1] >> 192.168.1
>>IN> Choose the first byte [Ex: 1] >> 1
>>IN> Choose the last byte [Ex: 254] >> 20
>>LOG> 192.168.1.1 >OK
>>LOG> 192.168.1.2 >NOK
>>LOG> 192.168.1.3 >NOK
>>LOG> 192.168.1.4 >NOK
>>LOG> 192.168.1.5 >NOK
>>LOG> 192.168.1.6 >NOK
>>LOG> 192.168.1.7 >NOK
>>LOG> 192.168.1.8 >NOK
>>LOG> 192.168.1.9 >NOK
>>LOG> 192.168.1.10 >NOK
>>LOG> 192.168.1.11 >NOK
>>LOG> 192.168.1.12 >OK
>>LOG> 192.168.1.13 >NOK
>>LOG> 192.168.1.14 >NOK
>>LOG> 192.168.1.15 >OK
>>LOG> 192.168.1.16 >NOK
>>LOG> 192.168.1.17 >NOK
>>LOG> 192.168.1.18 >NOK
>>LOG> 192.168.1.19 >NOK
>>LOG> 192.168.1.20 >NOK
>>RES> THE FOLLOWING ADDRESSES HAVE BEEN FOUND >>
192.168.1.1
192.168.1.12
192.168.1.15

>>INFO> RESULTS STORED IN [output/111029-23h04/N-192.168.1.1-20_M-all_NBNS.txt]
>>PRESS ANY KEY TO CONTINUE
```

Net2SharePwn

Readme

```
>>IN>Scan ARP[1], Scan NBNS[2], Scan TCP 139/445[3] >> 3
>>IN> Choose a network target [NMAP Format] >> 192.168.1.0/24
output/111029-23h04/N-192.168.1.0NET24_M-all_SMB.txt

Starting Nmap 5.35DC1 ( http://nmap.org ) at 2011-10-29 23:55 CEST
Warning: Unable to open interface vmnet1 -- skipping it.
Warning: Unable to open interface vmnet8 -- skipping it.
WARNING: Unable to find appropriate interface for system route to 172.16.177.254
Nmap scan report for 192.168.1.0
Host is up.
PORT    STATE    SERVICE
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds

Nmap scan report for livebox.home (192.168.1.1)
Host is up (0.0049s latency).
PORT    STATE  SERVICE
139/tcp open   netbios-ssn
445/tcp closed microsoft-ds
MAC Address: 7C:03:4C:62:90:CB (Unknown)
 ...

Nmap scan report for Maryse-TOSH.home (192.168.1.12)
Host is up (0.31s latency).
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
 ...

Nmap done: 256 IP addresses (256 hosts up) scanned in 284.07 seconds
>>INFO> RESULTS STORED IN [output/111029-23h04/N-192.168.1.0NET24_M-all_SMB.txt]
>>RES> THE FOLLOWING ADDRESSES HAVE BEEN IDENTIFIED >>
192.168.1.1
192.168.1.12
```

4a. Add/modify file containing UP HOSTS, manually (new option from 1.1b)

```
#################################################
>>IN> Choose your operation >> 4a
```

Objective >This function allows to add your own IP addresses through a new text file with a name well formatted Input >None Output > `N-<name>_M-all.txt`

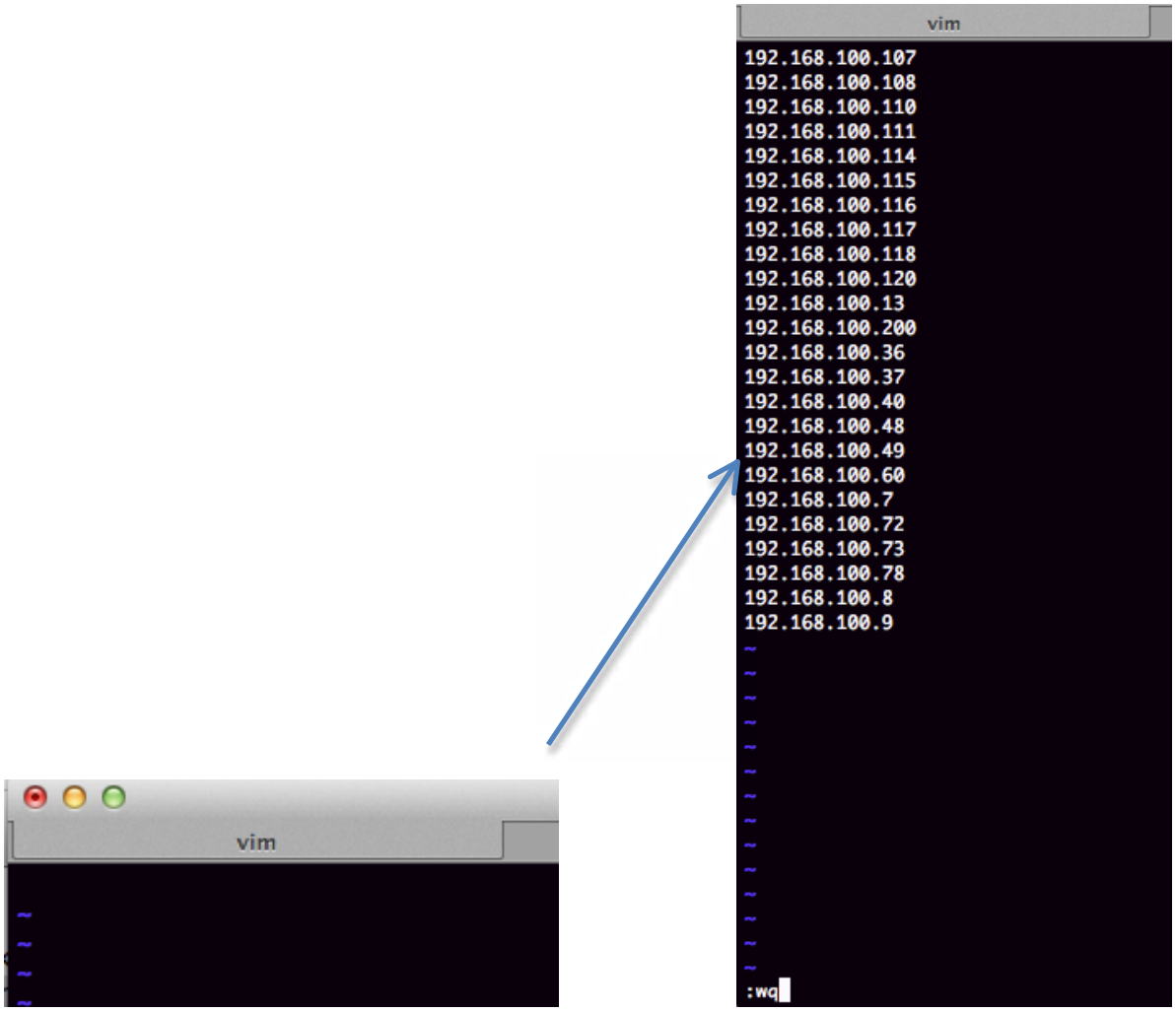
```
>>IN> Choose your operation >> 4a
>>INFO> The following lists of IP addresses are available >>
N-test_M-all.txt

This option allows to add or modify file containing ip addresses (one ip per line)
Type an existing <file name> or a new <file name> (N-<file name>_M-all.txt > test2
```

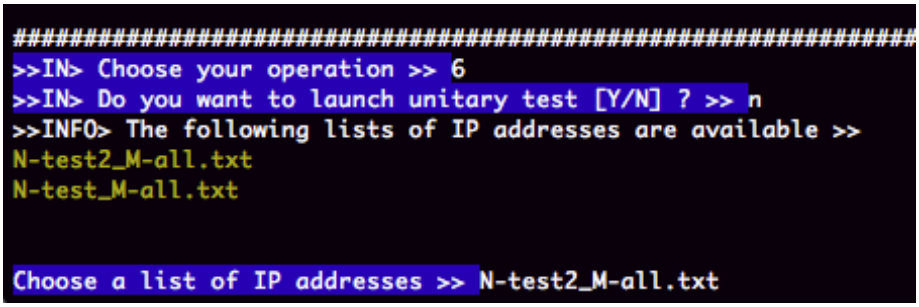
You can add your own IP addresses (vim)

Net2SharePwn

Readme

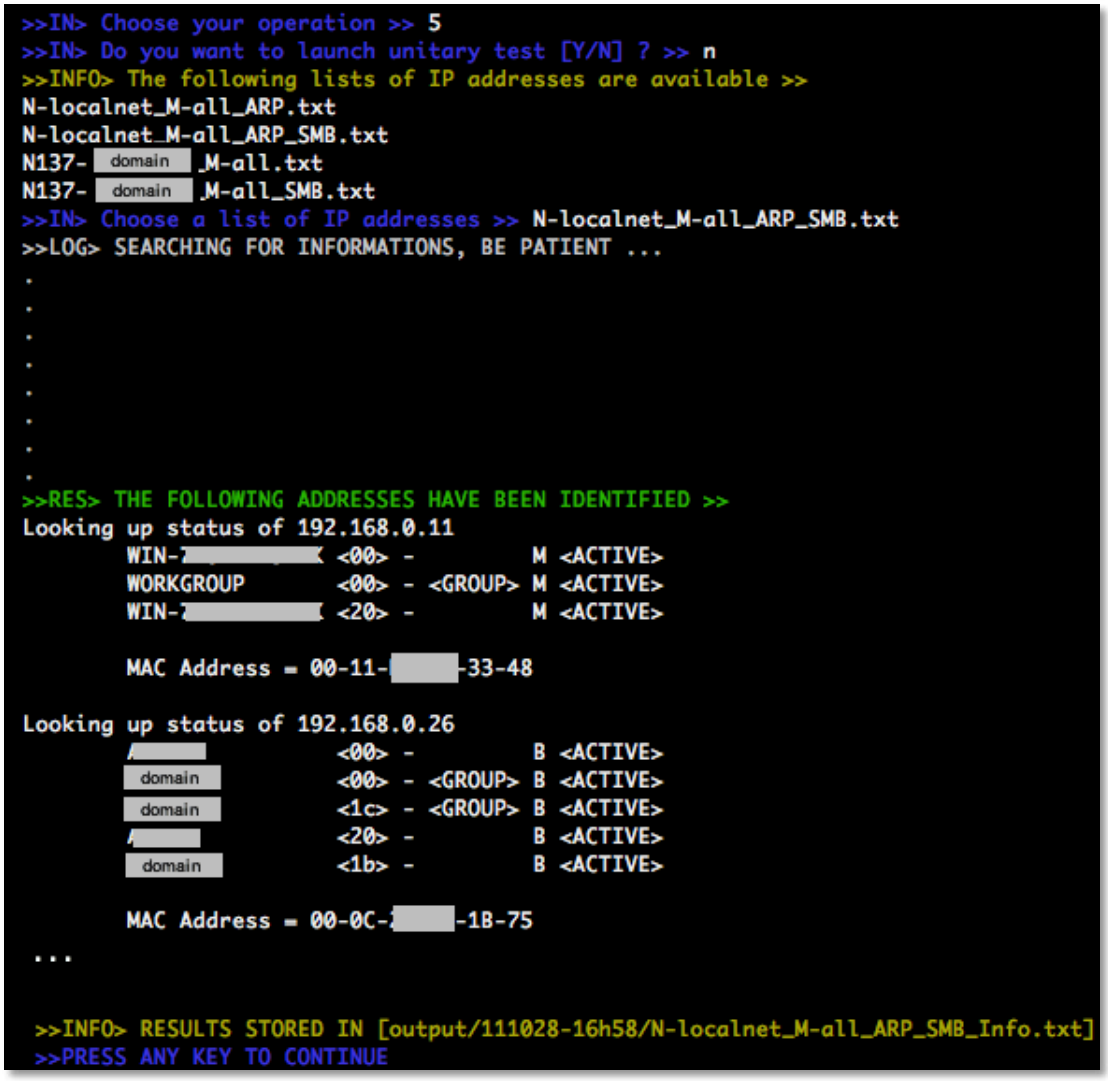


Next, you can select the newly created file to search information or network shares.



f. Generate SYSTEM INFORMATION

Objective >This function allows extracting NetBIOS information for one IP address or several IP addresses in order to identify their roles (nbstat or nbtscan scanning). This is used in the function "Find ACTIVE DIRECTORY servers".
Input >`N-<foobar>.txt` *OR one IP address*
Output >`N-<foobar>_Info.txt` *OR* *`IP-<YourIPAddress>_Info.txt`*



g. Find NETWORK SHARES

Objective >This function allows to find network shares available and mountable with your Windows privileges (anonymous, standard user, admin user, …) for one IP address or several IP addresses
Input >`N-<foobar>.txt` *OR one IP address*
Output >N-<foobar>`_S-all.txt` *OR* *`IP-<YourIPAddress>_S-all.txt`*

Net2SharePwn

Readme

```
>>IN> Choose your operation >> 6
>>IN> Do you want to launch unitary test [Y/N] ? >> n
>>INFO> The following lists of IP addresses are available >>
N- domain _M-all.txt
N-localnet_M-all_ARP.txt
N-localnet_M-all_ARP_SMB.txt
N-localnet_M-all_ARP_SMB_ADbyNBT.txt
N-localnet_M-all_ARP_SMB_Info.txt
N-localnet_M-all_ARP_SMB_S-all.txt
N137- domain _M-all.txt
N137- domain _M-all_SMB.txt
Choose a list of IP addresses >> N- domain _M-all.txt
>>TRACE>>172.16 7
timeout connecting to 172.16 7:445
Error connecting to 172.16 7 (Host is down)
>>RES > NO FOUND SHARE :(

>>TRACE>>172.16 1
Domain=[ domain ] OS=[Windows 7 Professional 7600] Server=[Windows 7 Professional 6.1]
>>RES>> NETWORK SHARE ADMIN$ OF 172.16 1 IS UNMOUNTABLE :(
>>RES>> NETWORK SHARE C$ OF 172.16 1 IS UNMOUNTABLE :(
>>RES>> NETWORK SHARE D$ OF 172.16 1 IS UNMOUNTABLE :(
>>LOG> [/Volumes/S-172.16 1] IS UNMOUNTED
>>RES>> NETWORK SHARE EVOA OF 172.16 1 IS MOUNTABLE ;)
>>LOG> [/Volumes/S-172.16 1] IS UNMOUNTED
>>RES>> NETWORK SHARE Logiciel OF 172.16 1 IS MOUNTABLE ;)
>>LOG> [/Volumes/S-172.16 1] IS UNMOUNTED
>>RES>> NETWORK SHARE share OF 172.16 1 IS MOUNTABLE ;)
>>TRACE>>172.16 7
timeout connecting to 172.16 7:445
...
>>INFO> RESULTS STORED IN [output/111028-16h58/N- domain _M-all_S-all.txt]
>>PRESS ANY KEY TO CONTINUE
```

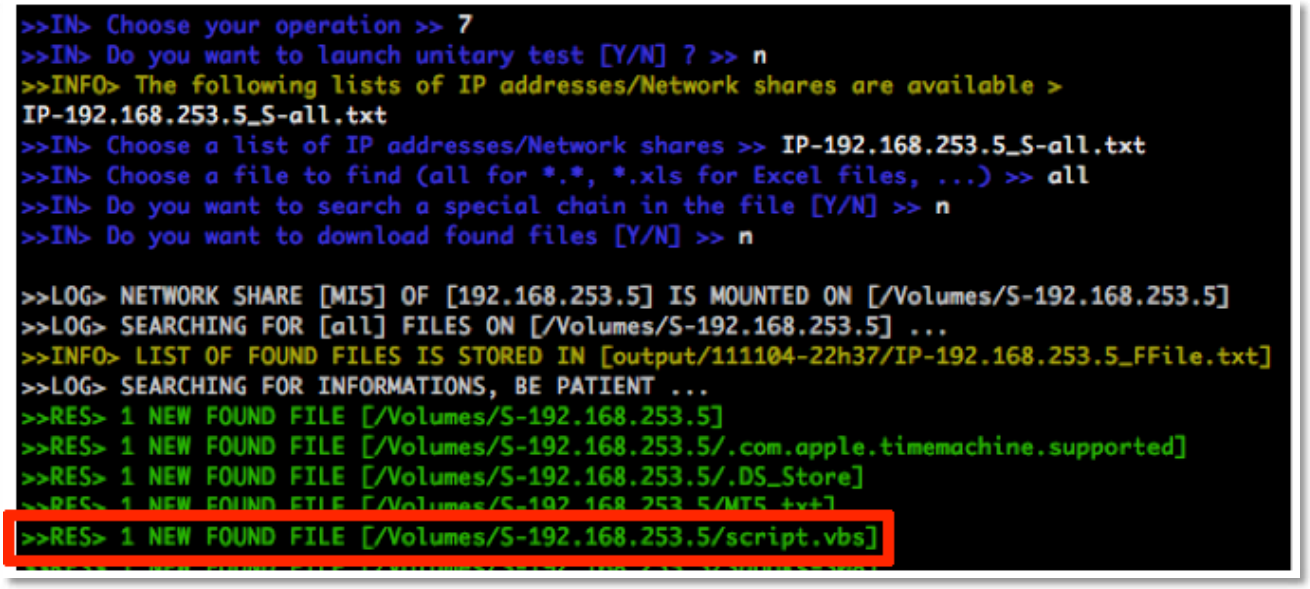
```
bash-3.2# more N- domain _M-all_S-all.txt
172.16. 1,  DA
172.16. 1,Logiciel
172.16. 1,share
172.16. 0,VM
172.16. 0,Data
172.16. 10,share
```

```
>>IN> Choose your operation >> 6
>>IN> Do you want to launch unitary test [Y/N] ? >> y
>>IN> Choose an IP address >> 192.168.253.5
>>TRACE>>192.168.253.5
Domain=[ARNHACK] OS=[Unix] Server=[Samba 3.0.28a-apple]
Domain=[ARNHACK] OS=[Unix] Server=[Samba 3.0.28a-apple]
>>LOG> [/Volumes/S-192.168.253.5] IS UNMOUNTED
>>RES>> NETWORK SHARE MIS OF 192.168.253.5 IS MOUNTABLE ;)
>>LOG> [/Volumes/S-192.168.253.5] IS UNMOUNTED
>>RES>> NETWORK SHARE Movies OF 192.168.253.5 IS MOUNTABLE ;)
>>RES>> NETWORK SHARE My OF 192.168.253.5 IS UNMOUNTABLE :(
>>LOG> [/Volumes/S-192.168.253.5] IS UNMOUNTED
>>RES>> NETWORK SHARE client_prox OF 192.168.253.5 IS MOUNTABLE ;)
>>RES>> NETWORK SHARE séries OF 192.168.253.5 IS UNMOUNTABLE :(
>>RES>> NETWORK SHARE tést OF 192.168.253.5 IS UNMOUNTABLE :(
>>INFO> RESULTS STORED IN [output/111103-23h45/IP-192.168.253.5_S-all.txt]
>>PRESS ANY KEY TO CONTINUE
```

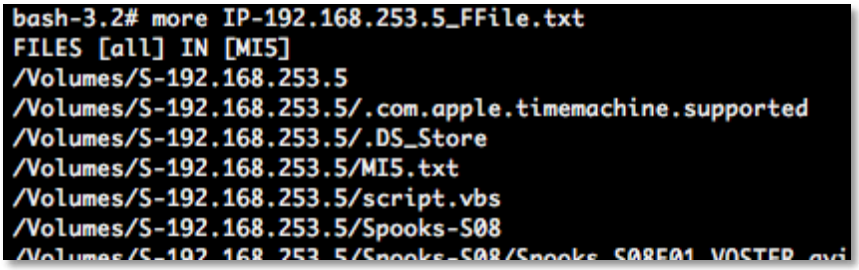
h. Find SPECIAL FILES from network shares

Objective >This function allows to search and/or download special files into mountable network shares. Special files can be identified from their extension (ex: “xls”) and their content (ex: “password”) Input >`N-<foobar>_S-all.txt` OR *`IP-<YourIPAddress>_S-all.txt`* Output > Logs of Found files (not downloaded) >`IP-<IPAddress>_FFile.txt` Logs of Downloaded files >`IP-<IPAddress>_DFile.txt` Directory containing downloaded files >`<YourProject>/DOWNLOADED-FILES/<YourIpAdress>/`

It’s possible to visualize ALL available files into network shares previously identified.



Found files can be visualized from “_FFile.txt”.



Next, it’s easy to download special files like scripts with the “VBS” extension and containing “password”,

Net2SharePwn

Readme

```
>>IN> Choose your operation >> 7
>>IN> Do you want to launch unitary test [Y/N] ? >> n
>>INFO> The following lists of IP addresses/Network shares are available >
IP-192.168.253.5_S-all.txt
>>IN> Choose a list of IP addresses/Network shares >> IP-192.168.253.5_S-all.txt
>>IN> Choose a file to find (all for *.*, *.xls for Excel files, ...) >> *.vbs
>>IN> Do you want to search a special chain in the file [Y/N] >> y
>>IN> Choose a special chain >> password
>>IN> Do you want to download found files [Y/N] >> y

>>LOG> NETWORK SHARE [MI5] OF [192.168.253.5] IS MOUNTED ON [/Volumes/S-192.168.253.5]
>>LOG> SEARCHING FOR [*.vbs] FILES ON [/Volumes/S-192.168.253.5] ...
>>INFO> LIST OF FOUND FILES IS STORED IN [output/111104-22h37/IP-192.168.253.5_DFile.txt]
>>LOG> SEARCHING FOR INFORMATIONS, BE PATIENT ...
>>RES> 1 NEW DOWNLOADED FILE [/Volumes/S-192.168.253.5/script.vbs]
>>INFO> COMPLETE DOWNLOAD - RESULTS STORED IN [output/111104-22h37/DOWNLOADED-FILES/192.168.253.5]
>>LOG> [/Volumes/S-192.168.253.5] IS UNMOUNTED

>>LOG> NETWORK SHARE [Movies] OF [192.168.253.5] IS MOUNTED ON [/Volumes/S-192.168.253.5]
>>LOG> SEARCHING FOR [*.vbs] FILES ON [/Volumes/S-192.168.253.5] ...
>>INFO> LIST OF FOUND FILES IS STORED IN [output/111104-22h37/IP-192.168.253.5_DFile.txt]
>>LOG> SEARCHING FOR INFORMATIONS, BE PATIENT ...
>>INFO> COMPLETE DOWNLOAD - RESULTS STORED IN [output/111104-22h37/DOWNLOADED-FILES/192.168.253.5]
>>LOG> [/Volumes/S-192.168.253.5] IS UNMOUNTED

>>LOG> NETWORK SHARE [client_prox] OF [192.168.253.5] IS MOUNTED ON [/Volumes/S-192.168.253.5]
>>LOG> SEARCHING FOR [*.vbs] FILES ON [/Volumes/S-192.168.253.5] ...
>>INFO> LIST OF FOUND FILES IS STORED IN [output/111104-22h37/IP-192.168.253.5_DFile.txt]
>>LOG> SEARCHING FOR INFORMATIONS, BE PATIENT ...
>>INFO> COMPLETE DOWNLOAD - RESULTS STORED IN [output/111104-22h37/DOWNLOADED-FILES/192.168.253.5]
>>LOG> [/Volumes/S-192.168.253.5] IS UNMOUNTED
```

and all files with the “EXE” extension.

```
>>LOG> NETWORK SHARE [client_prox] OF [192.168.253.5] IS MOUNTED ON [/Volumes/S-192.168.253.5]
>>LOG> SEARCHING FOR [*.exe] FILES ON [/Volumes/S-192.168.253.5] ...
>>INFO> LIST OF FOUND FILES IS STORED IN [output/111104-22h27/IP-192.168.253.5_F.txt]
>>LOG> SEARCHING FOR INFORMATIONS, BE PATIENT ...
>>RES> 1 NEW FOUND FILE [/Volumes/S-192.168.253.5/proxmark3_win_bins/bin/cli.exe]
>>RES> 1 NEW FOUND FILE [/Volumes/S-192.168.253.5/proxmark3_win_bins/bin/flasher.exe]
>>RES> 1 NEW FOUND FILE [/Volumes/S-192.168.253.5/proxmark3_win_bins/bin/proxmark3.exe]
>>RES> 1 NEW FOUND FILE [/Volumes/S-192.168.253.5/proxmark3_win_bins/bin/snooper.exe]
>>RES> 1 NEW FOUND FILE [/Volumes/S-192.168.253.5/proxmark3_win_bins/extra/nonce2key/nonce2key.exe]
```

Found and downloaded files can be visualized from “_DFile.txt”.

```
bash-3.2# more IP-192.168.253.5_DFile.txt
FILES [.vbs] STORING [password] IN [MI5]
/Volumes/S-192.168.253.5/script.vbs
FILES [.vbs] STORING [password] IN [Movies]
FILES [.vbs] STORING [password] IN [client_prox]
FILES [.vbs] STORING [password] IN [MI5]
/Volumes/S-192.168.253.5/script.vbs
FILES [.exe] IN [MI5]
FILES [.exe] IN [Movies]
FILES [.exe] IN [client_prox]
/Volumes/S-192.168.253.5/proxmark3_win_bins/bin/cli.exe
/Volumes/S-192.168.253.5/proxmark3_win_bins/bin/flasher.exe
/Volumes/S-192.168.253.5/proxmark3_win_bins/bin/proxmark3.exe
/Volumes/S-192.168.253.5/proxmark3_win_bins/bin/snooper.exe
/Volumes/S-192.168.253.5/proxmark3_win_bins/extra/nonce2key/nonce2key.exe
```

Next, the downloaded files can be visualized.

```
bash-3.2# ls -ls DOWNLOADED-FILES/192.168.253.5/
total 16
8 -rwxrwxrwx  1 _unknown  _unknown  139  4 nov 00:53 MI5.txt
8 -rwxrwxrwx  1 _unknown  _unknown   16  4 nov 00:50 script.vbs
```

```
>>IN> Choose your operation >> 13
>>IN> CMD (q pour quitter)>more output/111103-23h45/DOWNLOADED-FILES/192.168.253.5/script.vbs
password=test123
```

IMPORTANT: if you want to re-launch the download with a file type already tested, it's advised to delete the "_DFile.txt" via "`rm IP-<IPAddress>_DFile.txt`". It's a bug … sorry.

i. Find ACTIVE DIRECTORY servers

Objective >This function allows to identify, from Netbios information, Active Directory servers. Input >`N-<foobar>_Info.txt` OR *`IP-<YourIPAddress>_Info.txt`* Output >`N-<foobar>_ADbyNBT.txt` OR *`IP-<YourIPAddress>_ADbyNBT.txt`*

```
>>IN> Choose your operation >> 8
>>INFO> GENERATED INFORMATION FILES  >>
>>INFO> The following lists of information files are available >
N-localnet_M-all_ARP_SMB_Info.txt
>>IN> Choose a information file >> N-localnet_M-all_ARP_SMB_Info.txt
>>RES> IDENTIFIED AD SERVERS >>
192.168.0.26
>>RES> RESULTS STORED IN [output/111028-16h58/N-localnet_M-all_ARP_SMB_ADbyNBT.txt]
>>PRESS ANY KEY TO CONTINUE
```

Net2SharePwn

Readme

Supp. Functions

a. Find Windows NetBIOS names of WORKSTATIONS and SERVERS (debug mode)

Objective > This debug function allows identifying the NetBIOS workstations and servers names belonging to a special Windows domain or workgroup. This function is very verbose and can allow extracting interesting network information.
Input >`D-all.txt`
Output >`D-all_M-all_verbose.txt`

```
>>IN> Choose your operation >> 2b
>>LOG> SEARCHING FOR WINDOWS NETBIOS NAMES (verbose mode), BE PATIENT ...
>>INFO> RESULTS STORED IN [output/111028-23h12/D-all_M-all_verbose.txt]
>>PRESS ANY KEY TO CONTINUE
```

b. Find IP address from 2b

Objective >Fromthe previously verbose command, it is possible to identify IP addresses of isolated Workstations for example.
Input >`D-all_M-all_verbose.txt`
Output > Not stored and just screened

c. Check NetBIOS and SMB services

Objective >This function allows launching TCP port scanning on IP addresses and NetBIOS and SMB ports. This function is very useful to avoid attempting connections on network shares while SMB or Netbios service is not available.
Input >`N-<foobar>.txt`
Output >`N-<foobar>_SMB.txt`

```
>>IN> Choose your operation >> 3c
>>INFO> The following lists of IP addresses are available >>
N-localnet_M-all_ARP.txt
N-localnet_M-all_ARP_SMB.txt
N137- domain _M-all.txt
N137- domain _M-all_SMB.txt
>>IN> Choose a file of IP Addresses >> N-localnet_M-all_ARP.txt
>>IN> Do you want to delete the previous results [Y/N] ? >> y
 ...
Nmap scan report for 192.168.0.11
Host is up (0.0072s latency).
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap scan report for 192.168.0.10
Host is up (0.0033s latency).
PORT    STATE  SERVICE
139/tcp closed netbios-ssn
445/tcp closed microsoft-ds
 ...

Nmap done: 25 IP addresses (19 hosts up) scanned in 8.98 seconds
>>RES> THE FOLLOWING ADDRESSES HAVE BEEN IDENTIFIED >>
192.168.0.11
192.168.0.26
192.168.0.32
192.168.0.30
192.168.0.31
192.168.0.200
192.168.0.212
192.168.0.233

>>INFO> RESULTS STORED IN [output/111028-16h58/N-localnet_M-all_ARP_SMB.txt]
```

Net2SharePwn

Readme

Tools

a. Check the connection to a NETWORK SHARE

Objective >This function allows to check if your Windows privileges (anonymous, standard user, admin user, …) allow to mount a special network share Input >One IP address, name of a network share Output >Not stored and just screened

```
>>IN> Choose your operation >> 9
>>IN> Choose an IP address >> 192.168.253.5
>>IN> Choose a network share name >> MI5
>>LOG> [/Volumes/S-192.168.253.5] IS UNMOUNTED
>>RES> NETWORK SHARE [MI5] OF [192.168.253.5] CAN BE MOUNTED
>>PRESS ANY KEY TO CONTINUE
```

```
>>IN> Choose your operation >> 9
>>IN> Choose an IP address >> 192.168.253.5
>>IN> Choose a network share name >> séries
>>RES> IMPOSSIBLE TO MOUNT [séries] OF [192.168.253.5]
>>PRESS ANY KEY TO CONTINUE
```

b. Mount and unmount a NETWORK SHARE

Objective >>This function allows to (un)mount a special network share Input >One IP address, name of a network share Output >Not stored and just screened

```
>>IN> Choose your operation >> 10
>>IN> Choose an IP address >> 192.168.253.5
>>IN> Choose a network share name >> MI5
>>LOG> NETWORK SHARE [MI5] OF [192.168.253.5] IS MOUNTED
>>IN> Do you want to unmount this network share [Y/N] ? >>
```

```
arnhack:/ sudoman$ sudo bash
Password:
bash-3.2# ls -ls /Volumes/S-192.168.253.5/
total 82
14 -r--r--r--@  1 root  wheel   6148 29 oct 23:03 .DS_Store
 0 -r--r--r--   1 root  wheel      0 18 sep 00:50 .com.apple.timemachine.supported
 2 -r--r--r--   1 root  wheel    139 26 mar  2011 MI5.txt
32 dr-xr-xr-x  10 root  wheel  16384 26 mar  2011 Spooks-S08
32 dr-xr-xr-x  13 root  wheel  16384 13 avr  2011 Spooks-S09
 2 -r--r--r--@  1 root  wheel     16 30 oct 23:44 script.vbs
```

```
>>IN> Do you want to unmount this network share [Y/N] ? >>y
>>LOG> [/Volumes/S-192.168.253.5] IS UNMOUNTED
>>PRESS ANY KEY TO CONTINUE
```

c. NEW or LOAD PROJECT

Objective >This function allows to create a new project or to load an existing project without quitting Net2SharePwn. Moreover, you can use this function to change your privilege level (from anonymous to authenticated user) Input >None Output >None

```
>>IN> Choose your operation >> 11
>>IN> Have you got Windows credentials, [Y/N] ? >> y
>>LOG> File auth/smb-auth.txt exists
username=DEVOTEAM\toto
>>LOG> File auth/smb-auth2.txt exists
username=toto
workgroup=DEVOTEAM
>>IN> Do you want load a special project, [Y/N] ? >> y
>>INFO> AVAILABLE PROJECTS :
111028-16h58    111028-17h25
>>IN> Choose your project >> 111028-16h58
#########################################################################
                                <<< MAIN : output/111028-16h58>>>
                                <<< CRED : YES >>>
```

d. Change Windows CREDENTIALS

Objective >This function allows to change credentials if you chose to launch Net2SharePwn with authentication (not anonymous) Input >Domain, username and password Output >`auth/smb-auth.txt, auth/smb-auth2.txt`

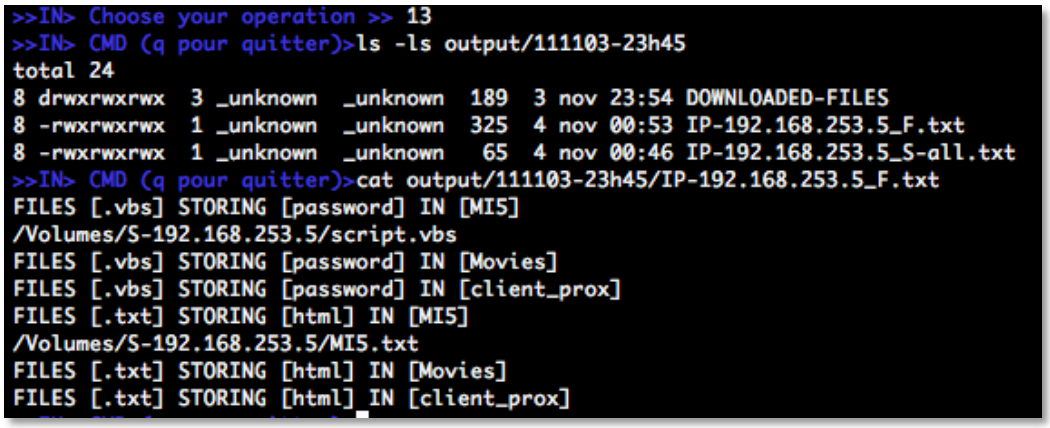
```
>>IN> Choose your operation >> 12
>>IN> Choose domain (. if you do not know it) > TEST
>>IN> Choose username > sudoman
>>IN> Choose password > P@ssWor33&
>>LOG> Credentials in auth/smb-auth.txt >
#####################################
username=TEST\sudoman
password=P@ssWor33&
#####################################
>>LOG> Credentials in auth/smb-auth2.txt >
#####################################
username=sudoman
password=P@ssWor33&
workgroup=TEST
#####################################
```

e. EXECUTE system commands

Objective >This function allows to execute system commands from Net2SharePwn without having to open another terminal Input >Your commands Output >Commands result

Net2SharePwn

Readme



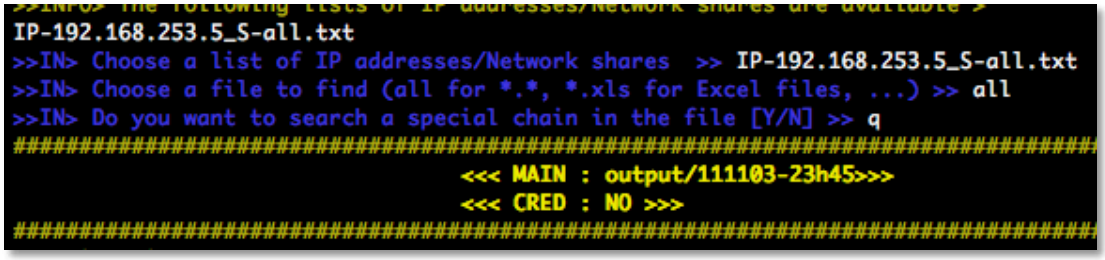
Net2SharePwn

Readme

Internal functions

a. Quit

For some functions, it is possible to come back to the main menu by typing “q”.



Net2SharePwn

Readme

Known limitations

B2 : On Moutain Lion, ”mount_smbfs” is very slow to mount and unmounts network share

Net2SharePwn

Readme

About me

I'm a French security auditor and pentester for XMCO. I have almost 7 years of experience in the security domain.

- Personal E-mail: sganama[at]gmail[dot]com
- Personal Blog: http://sud0man.blogspot.com
- Linkedin: http://fr.linkedin.com/pub/arnaud-malard/2/416/a05