

Introducing weaknesses into security devices

Tuning to a different key!

Arron “finux” Finnon

#BerlinSides - 29/12/11



Summary

Lets have a look at a VERY famous “exploit”, a VERY famous “Exploit Framework” and a VERY “famous” security device.

The issue I'm highlighting is;
A highly bespoke transmission method with a particular idiosyncrasy is being used. Hardly anyone has noticed!!!

I really tried not to make this talk a rant, but I failed.

Outline

- ◆ I could be proper grown up but I'm not going to
- ◆ Set a scene and tell you a tale
- ◆ Show you some captures
- ◆ Talk about why this works or doesn't work
- ◆ Rant a little bit about snake oil
- ◆ Probably offend some of you
- ◆ In fact if this goes right I should upset all of you

My views

- ◆ The only time you should you use an evasion technique is when you ask for it
- ◆ That you should never run software on the wire without knowing WTF it does
- ◆ That MSF is the Windows of hacking
- ◆ You should never run an exploit WITHOUT a capture running
- ◆ IDS/IPS vendors talk throughput not detection rates!

WHOAMI

- ◆ Damn good question!!!!
 - Security Researcher
 - IDAPPCOM
 - Used to be freelance
 - Seem to have spoken a lot recently
 - Podcaster
 - Into the whole “freetard” community BS
 - Hated by ALL prefects from an early age

MS08-067

- ◆ If you have no idea what this is, go to the bar grab a drink we'll be finished in about an hour.
- ◆ If it helps every h@x0r at a conference does some MSF related demo with it
- ◆ In short; very nasty exploit which gives remote code execution against MS boxes
- ◆ Even shorter: WTF, UMADBRO!!!!!!!!!!

finux – how did you get here?

- ◆ Undertook a project to document 40 known IDS evasion techniques
- ◆ Was in the church of “Metasploit”! Thought it was the tool of “CHAMPIONS”
- ◆ I spent x3 days staring at captures questioning my very own sanity
- ◆ On a side note; I once stared into the directory structure and it self-referenced me back.

Metasploit

The Metasploit Project is an "Open Source" security project, its aim is to provide information about vulnerabilities and to assist penetration testers with security assessments.

There can be little doubt of Metasploit's wide spread popularity within the security community. InfoSecurity Magazine recently reported (10/10/12) that Metasploit is estimated to have a 125,000 users.

Its now a commercial tool, paid for by venture capitalism

Best SE I've ever seen though, getting VC's to pay for something they could have downloaded for free

DCERPC::smbpipeio

“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

The “idiosyncrasy”

The term 'idiosyncrasy' seems the most appropriate to describe the transmission evasion/error within Metasploit. However the real issue is two-fold; Very few people are aware of the bespoke delivery method.

That Metasploit is very popular amongst the security industry professional.

So your going to ask this: Why you not turn it off?

All I can say is try it

The “captures” never lie!

- ◆ Okay here's x3 captures
- ◆ One with RW
- ◆ One with Trans
- ◆ And One that DOES NOT use MSF

I wish the tale stopped here...

- ◆ Why oh why does the god “Metasploit” hate me!
 - Because I know he uses evasion techniques without telling you
 - Because I know he does not always write code
 - SMB::pipe_evasion
 - ASK ME TO SHOW YOU THE LOLZ
 - Because I know that using MSF requires you to capture and analyse ANY exploit
 - SIDENOTE ask me about TCP::max_send_size

So my thoughts at the time....

- ◆ I love having an EXPLOIT framework
 - However as a “freetard” I feel let down
 - You get what you pay for – trollololol
- ◆ That I know that certain independent labs will now be running MSF and alternative PoC
 - Thank god, I feel I made a difference
 - I hope you guys will run Wireshark every time you run an exploit
- ◆ Its not an “evasion” technique if its on by default

What I can talk about

◆ SNORT

- Because talking about a certain “company” that “hypothetically” lifted code and implemented the same god damn transmission bugs would be pointless.
- Because if that did happen I certainly “couldn't talk about it”
- So to be clear – I am not talking about a vendor that has tried to grab a lot of attention!!!
 - Did I mention I like beer

Yo SNORT umadbro?

- ◆ VRT I love you but FFS WTF are you on?
 - Its not a 0day protection if you thought it was something else.
 - Normally when you misdiagnose something you don't write a paper saying how AWESOME you are
 - You have over cooked the pot
 - Finux's little tip
 - Drop anything that has a WRITE followed by an immediate READ

So here's the question!

- ◆ Did we introduce a weakness into security devices?
 - Yes we did
 - Well I didn't and you didn't, but we all played a part

- ◆ What would we have said to a customer that did the same thing?
 - How do we model this threat;
 - our egos
 - not eating our own dog food
 - Emperor's new clothes

Okay any other vendors affected?

◆ Er officially SNORT

- Basically though, if you only use MSF to test shit, your finished. Sorry its just the way it is
- You should have diversified

◆ Some one could do a test for me

- There is a “product” that has a buffer of a 1000 threats – I wonder if they use MSF for their samples?
- Lulz deep packet inspection

So heart on sleeve time!

- ◆ If we don't shape up its OVER
 - We only need another 50 days of lulz
 - Britain will end up like Germany
 - i.e. We'll stop port scanning
 - “Yo bro NMAP is illegal” - not be long
 - Because that ANTI-APT shit will come back and bite
 - We have sold millions of pounds of products that don't work
 - Any other industry this would be fraud

What else is a f**king joke!

- ◆ Because we're not testing IDS/IPS
 - Did I mention we're not testing IDS/IPS
 - You know what else no one tests IDS/IPS
- ◆ How the F**k can you protect, if you don't practice
 - You “pen test” infrastructure
 - Errr when did your security device stop being infrastructure
- ◆ Did I mention that no one is testing IDS/IPS?
 - I hope you have gotten the hint

Now time to look closer to home

- ◆ How can you blame MSF for this?
 - I can't, I blame YOU!
 - I actually read a paper from a VRT that talks about this and missed the GOD DAMN POINT
- Its time you start taking the burden off snake oil salesmen
 - Test their claims
- Stop believing in the hype
 - Vendor and Hacker Hype

Conclusion 1/2

- ◆ That 6 months of IDS research has made me:
 - ANGRY
 - RANT A LOT
 - HATE SECURITY
 - LOVE SECURITY
 - CONFUSED

While I'm here

- ◆ Okay now here's some IDS hackers war stories
 - UTM
 - Er so you need to scan the box to protect it
 - What you need to reassemble you can evade
 - Traffic normalization
 - Pfft more like protololololololol

Dangers of “character” matching



The “Butthead” Evasion Technique

This should be taken as seriously as the SNORT signature that inspired it.

SID1239 – WTF!!!!

- ◆ Rain Forest Puppy – May 2000 – RFPalyze
- ◆ Based on exploit found in the wild – Whisper
- ◆ CVE-2000-0347 – I know its old

Exploit

- ◆ So long story short
 - 95 && 98 will freak out when a malformed NetBIOS session request is received
- ◆ RFP basically attacked the messenger service with a message from BEAVIS that said yep yep
- ◆ He actually hard-coded it into the PoC

Rule:

- ◆ alert tcp \$EXTERNAL_NET any -> \$HOME_NET 139
(msg:"NETBIOS RFPalyze 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!!!!!!!

So let me get this right!



++



So “what if?”



++



So “what if?”



++



Real issue

- ◆ Whisper doesn't have BEAVIS or Yep, Yep
- ◆ SID1239 ONLY protects against an unmodified RFPalyze
 - Example of patching PoC not exploitation
- ◆ Trivial to bypass == false sense of security

errrrr

- ◆ "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA" – SID1394 (rev12 – WTF!!! o'rly)
- ◆ "CCCCCCCCCCCCCCCCCCCCCCCCCCCCCC" – SID1390 (rev8 – Still WTF doodz!!!!)
- ◆ Consider changing your email signatures to include these strings. Enough False-Positives should prove the point

Matching “Characters”



== BAD!!!!

Conclusion 2/2

- ◆ When bored read SNORTS rule sets
 - It always cheers me up
- ◆ How many “VENDORS” just put SNORT rules into their product
- ◆ Guess what we're not testing Detection Systems
- ◆ That 90's called and they want their frag, flag and port tricks back

Contact

- ◆ Twitter = f 1 n u x
- ◆ finux@finux.co.uk
- ◆ www.finux.co.uk
- ◆ www.idappcom.com

Questions

- ◆ Watch this space some papers are coming out next year