English Shellcode

Mason, Small, Monrose, MacManus

Presentation by:
Will Whiteside

What?

- This paper describes a technique to encode shellcode as syntactically correct sentences.

Why?

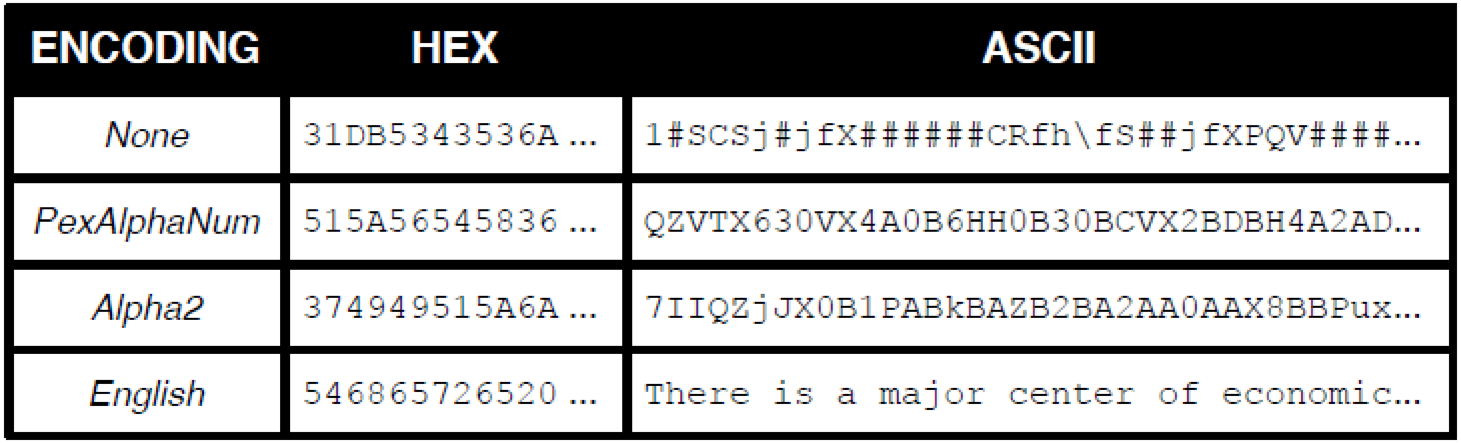
- It is impossible to tell the difference between syntactically correct English text that represents shellcode and syntactically correct English text that doesn't without much more semantic information.
- This level of semantic information would be properly categorized as strong AI.

Why?

- If we have an exploit that allows us to execute code sent separately from the exploit, English shellcode allows the shellcode to be delivered safely and under the radar for most IDS systems.

Previous work?

- There are several programs that convert arbitrary shell code into a representation that only uses a restricted character set.
- Two examples of this are given:



ENCODING	HEX	ASCII
None	31DB5343536A …	1#SCSj#jfX######CRfh\fS##jfXPQV####…
PexAlphaNum	515A56545836 …	QZVTX630VX4A0B6HH0B30BCVX2BDBH4A2AD…
Alpha2	374949515A6A …	7IIQZjJX0B1PABkBAZB2BA2AA0AAX8BBPux…
English	546865726520 …	There is a major center of economic…

Why is this better?

- While those other examples of shell code are only composed of letters and numbers, they do not correspond to even the simplest representations of English.
- The frequency of letters is completely off from what would be expected.
- Dictionary checks choke on this (we'd expect to be able to extract the language from a block of text)

Ok, so we want to have proper English. How?

- Some English sentences parse as valid shell code.
- The paper gives the silly example “Shake Shake Shake!” which parses as

```
push %ebx

push "ake "

push %ebx

push "ake "

push %ebx

push "ake!"
```

Ok, That's helpful....

- Yep, sure is.

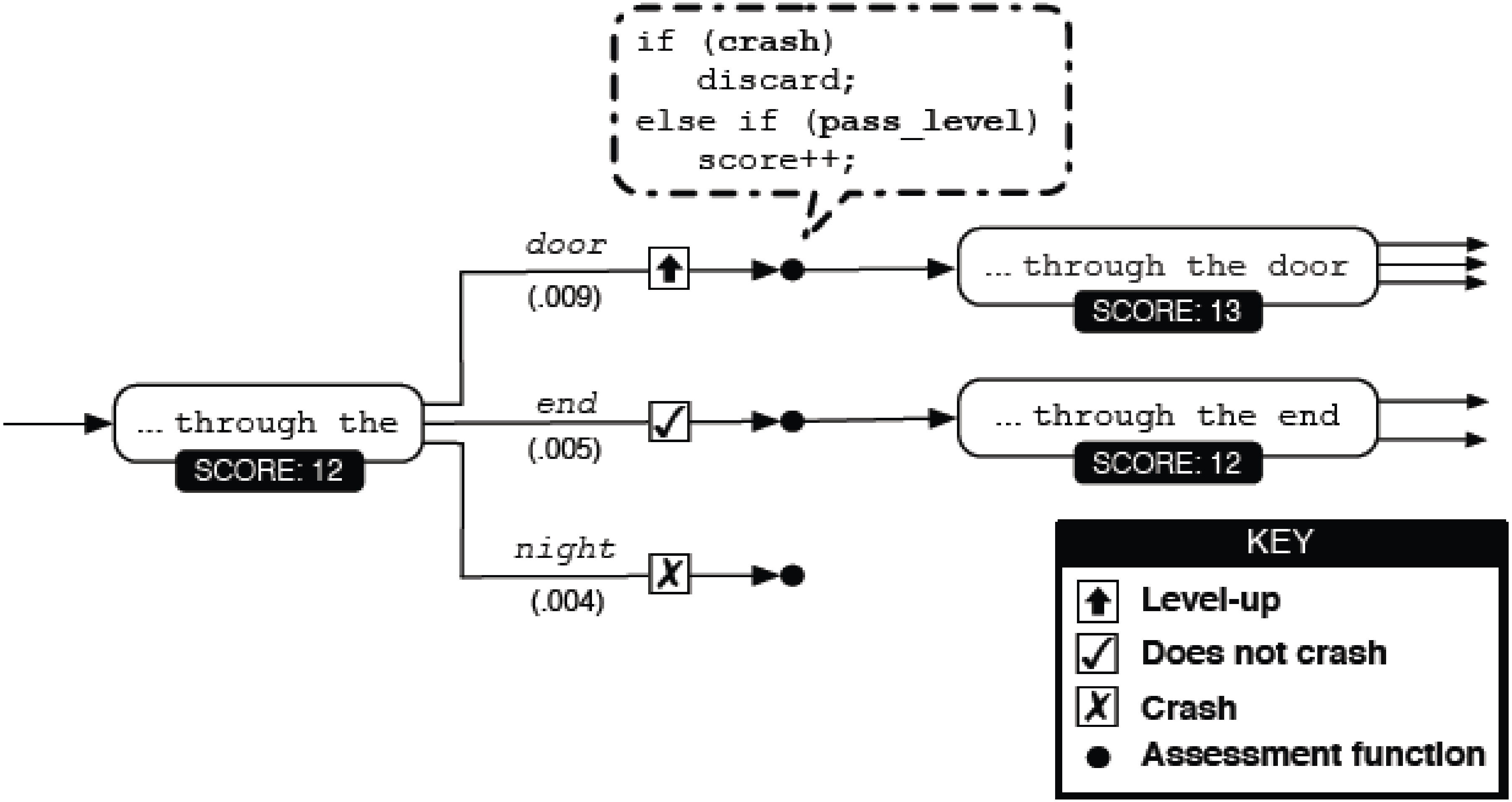
Quit kidding, how are we going to find some text that does what we want?

- We find a decoder that is a syntactically correct sentence.
- This decoder should be able to decode (and by inversion encode) any shell code.

How do we search?

- Sample words from the corpus, assemble them based on a statistical representation derived from the corpus, preferring search paths that have done well so far.

How about some great graphics?



```
if (crash)
   discard;
else if (pass_level)
   score++;
```

... through the

SCORE: 12

door (.009)

end (.005)

night (.004)

... through the door

SCORE: 13

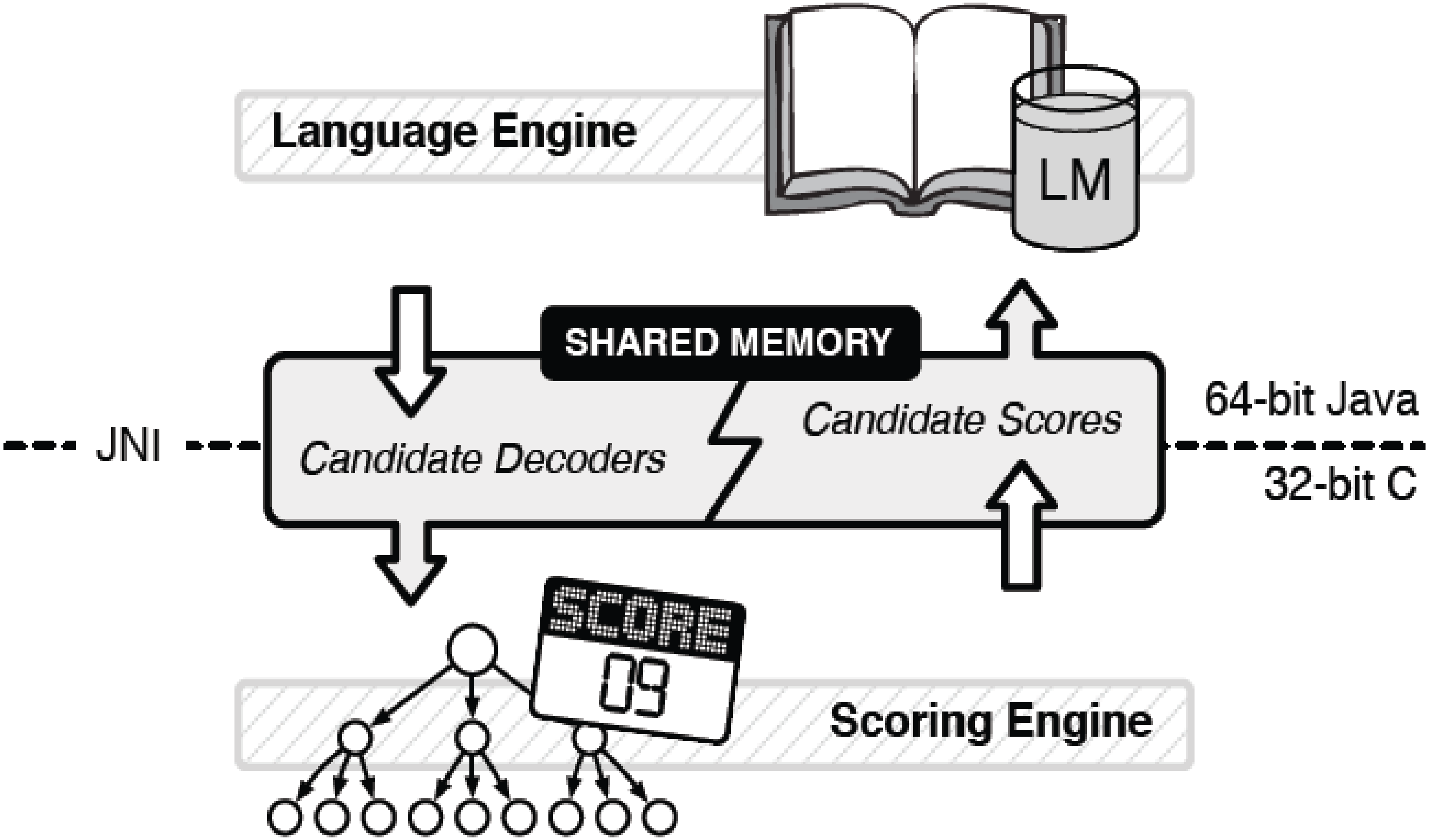
... through the end

SCORE: 12

KEY

- ⬆ Level-up
- ✓ Does not crash
- ✗ Crash
- ● Assessment function

Some more graphics



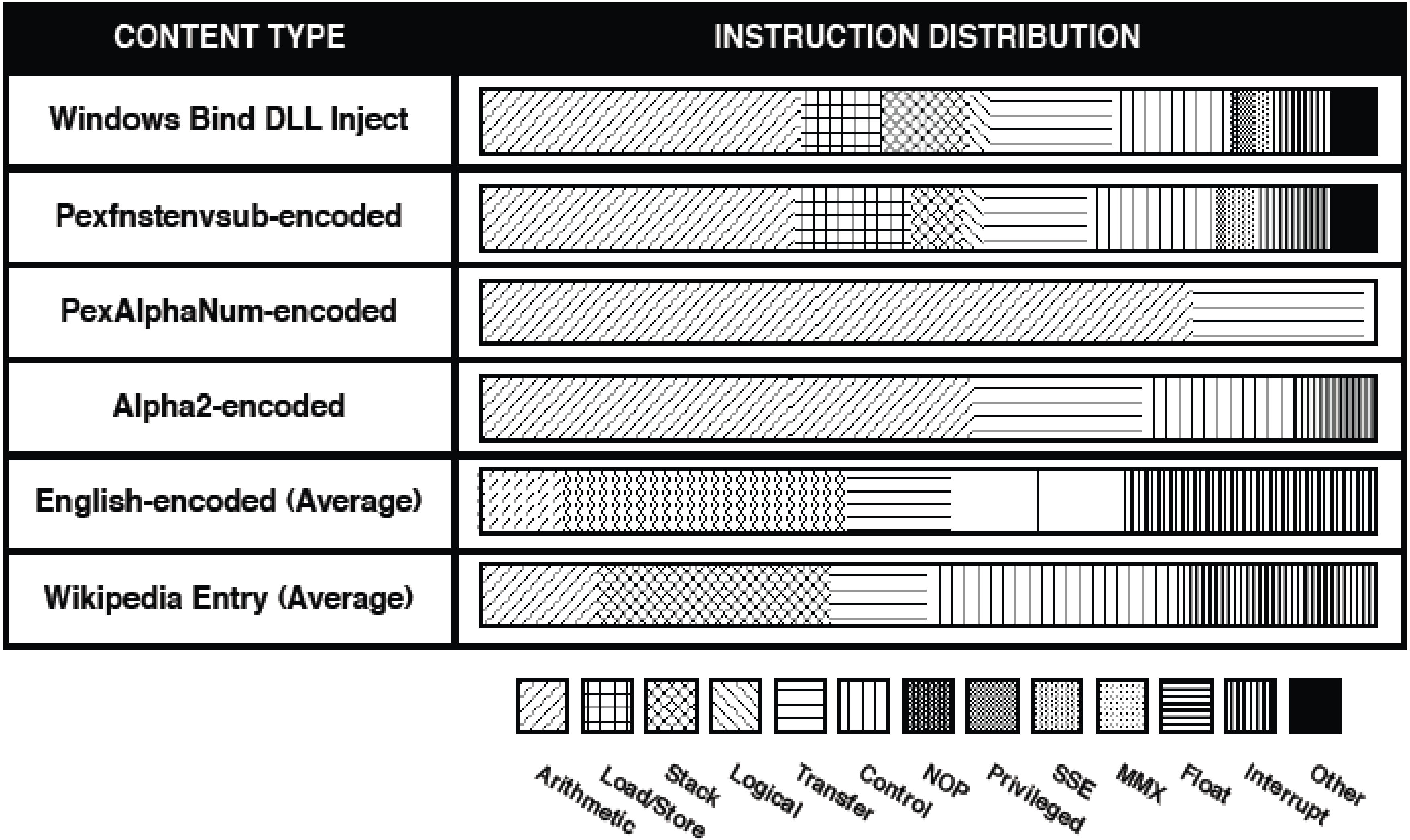
How difficult is it?

- These are extremely difficult to produce.
- There's about a page of difficulties they encountered in implementing a search strategy for these shell code sections.

How well does this work?

- The initial encoding takes a large amount of time.
- Aside from that, the English shellcode is Turing-Complete.
- There's no discussion of the length that encoding adds.

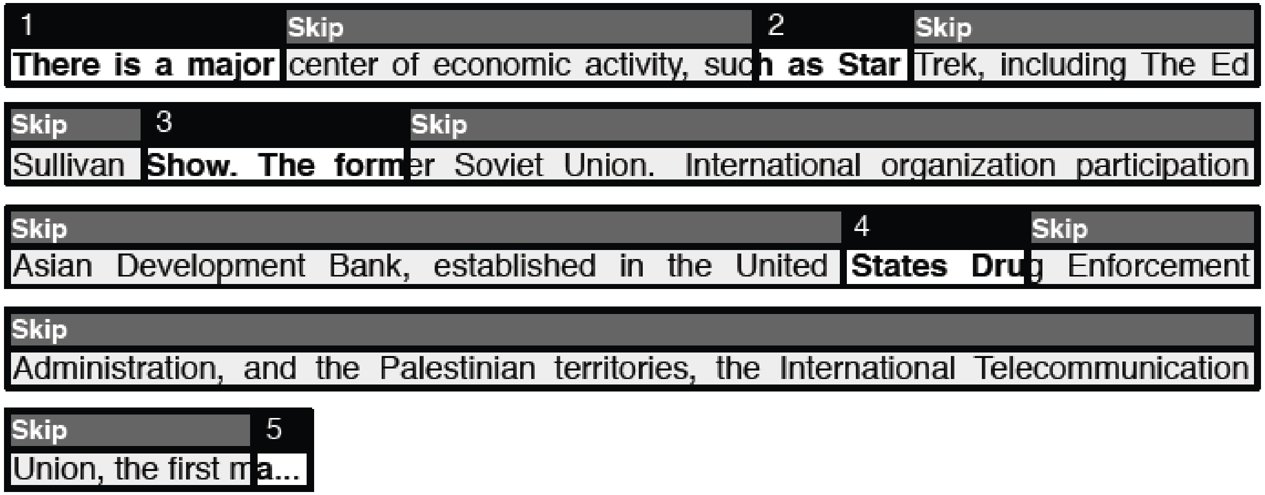
How detectable is it?



What does that mean?

- Good question.
- Superficially, it means that the encoded shellcode does not look like an executable when disassembled
- Not that this actually means anything.

	ASSEMBLY	OPCODE	ASCII
1	push %esp push $20657265 imul %esi,20(%ebx),$616D2061 push $6F *jb short $22*	54 68 65726520 6973 20 61206D61 6A 6F *72 20*	There is a major
2	push $20736120 push %ebx je short $63 *jb short $22*	68 20617320 53 74 61 *72 20*	h as Star
3	push %ebx push $202E776F push %esp push $6F662065 *jb short $6F*	53 68 6F772E20 54 68 6520666F *72 6D*	Show. The form
4	push %ebx je short $63 je short $67 jnb short $22 inc %esp *jb short $77*	53 74 61 74 65 73 20 44 *72 75*	States Dru
5	popad	61	a



1
Skip
2
Skip
There is a major
center of economic activity, suc
h as Star
Trek, including The Ed
Skip
3
Skip
Sullivan
Show. The form
er Soviet Union. International organization participation
Skip
4
Skip
Asian Development Bank, established in the United
States Dru
g Enforcement
Skip
Administration, and the Palestinian territories, the International Telecommunication
Skip
5
Union, the first m
a...

That's your evidence

- Yep.
- Notice that large sections of that text are skipped, these correspond to “instructions” that are completely ignored, yet are disassembled for that chart about how different the English shellcode is.

A valid measurement of difference.

- The method that is used to derive the text from the corpus means that an in-order statistical analysis would not be able to determine any difference from this or normal text.
- A good measurement would be sentence length, shallow semantic analysis, or chunking.
- Chunking, in particular, is a short set of rules to which almost all English (spoken, written, or even scribbled) conforms, if the shellcode cannot be chunked, then it could be detected in O(n) time.

Conclusion

- This paper shows that natively executable code need not be different in any major way from English, and that most payload examination methods would fail to detect such code.
- This represents a major flaw in IDS. This type of shellcode cannot be detected, so arbitrary code can be transmitted through an IDS. IDSs can still detect specific exploits, but the code may pass without interuption.

Questions?