University of BRISTOL

Return Oriented Programming

Sanjay Rawat

bristol.ac.uk

The Idea

Preventing the introduction of *malicious code* is sufficient to prevent the introduction of *malicious computation.. hmmmm.....!!!*

The Idea

Preventing the introduction of *malicious code* is sufficient to prevent the introduction of *malicious computation.. hmmmm.....!!!*

- Not the new attacking technique as such!
- Attack vector is different.
- Instead of passing shellcode, generate it.
- You still require to change the control flow => you still need to overflow something to start with!!
- Useful under non-executable stack and W(+)X

The Intuition behind ROP

- Lets visit past
  - Security of information is not new.
  - Internet gave new means of security attacks and thus new measures to address.
  - Cryptography and Steganography are much older techniques.
  - One among the older crypto systems is:

The Intuition....

The Intuition....

- Alan and Bob wants to exchange a msg.

The Intuition....

- Alan and Bob wants to exchange a msg.
- They make use of a news paper (book)!!

The Intuition....

- Alan and Bob wants to exchange a msg.
- They make use of a news paper (book)!!
- The same news paper (book) is available to both.

The Intuition....

- Alan and Bob wants to exchange a msg.
- They make use of a news paper (book)!!
- The same news paper (book) is available to both.
- There are plenty of sentences and words!!

The Intuition....

- Alan and Bob wants to exchange a msg.
- They make use of a news paper (book)!!
- The same news paper (book) is available to both.
- There are plenty of sentences and words!!
- The key is the set of offsets of words in a news article.

The Intuition

The commander of a group of Syrian army defectors retracted earlier claims that his followers launched an unprecedented attack inside the capital, Damascus, in an embarrassing turnaround for an armed movement trying to oust President Bashar Assad’s regime. lso Monday, Syrian soldiers opened fire on three Turkish buses, injuring two people, one of the bus drivers said. The attack occurred near the central city of Homs early Monday. Surmeli said he heard that two other Turkish buses had come under attack and another passenger was injured. They were able to cross into Turkey, he said. Syria has banned most foreign journalists from entering Syria and prevented the media from moving freely in the country.

This is only for example to show the seriousness. Author is not responsible for any future usage.

The Intuition

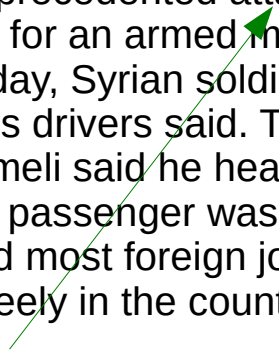
The commander of a group of Syrian army defectors retracted earlier claims that his followers launched an unprecedented attack inside the capital, Damascus, in an embarrassing turnaround for an armed movement trying to oust President Bashar Assad’s regime. lso Monday, Syrian soldiers opened fire on three Turkish buses, injuring two people, one of the bus drivers said. The attack occurred near the central city of Homs early Monday. Surmeli said he heard that two other Turkish buses had come under attack and another passenger was injured. They were able to cross into Turkey, he said. Syria has banned most foreign journalists from entering Syria and prevented the media from moving freely in the country.

19 35 103 55 45 68

This is only for example to show the seriousness. Author is not responsible for any future usage.

The Intuition

The commander of a group of Syrian army defectors retracted earlier claims that his followers launched an unprecedented attack inside the capital, Damascus, in an embarrassing turnaround for an armed movement trying to oust President Bashar Assad’s regime. lso Monday, Syrian soldiers opened fire on three Turkish buses, injuring two people, one of the bus drivers said. The attack occurred near the central city of Homs early Monday. Surmeli said he heard that two other Turkish buses had come under attack and another passenger was injured. They were able to cross into Turkey, he said. Syria has banned most foreign journalists from entering Syria and prevented the media from moving freely in the country.



19 35 103 55 45 68

This is only for example to show the seriousness. Author is not responsible for any future usage.

The Intuition

The commander of a group of Syrian army defectors retracted earlier claims that his followers launched an unprecedented attack inside the capital, Damascus, in an embarrassing turnaround for an armed movement trying to oust President Bashar Assad’s regime. lso Monday, Syrian soldiers opened fire on three Turkish buses, injuring two people, one of the bus drivers said. The attack occurred near the central city of Homs early Monday. Surmeli said he heard that two other Turkish buses had come under attack and another passenger was injured. They were able to cross into Turkey, he said. Syria has banned most foreign journalists from entering Syria and prevented the media from moving freely in the country.

19 35 103 55 45 68

This is only for example to show the seriousness. Author is not responsible for any future usage.

The Intuition

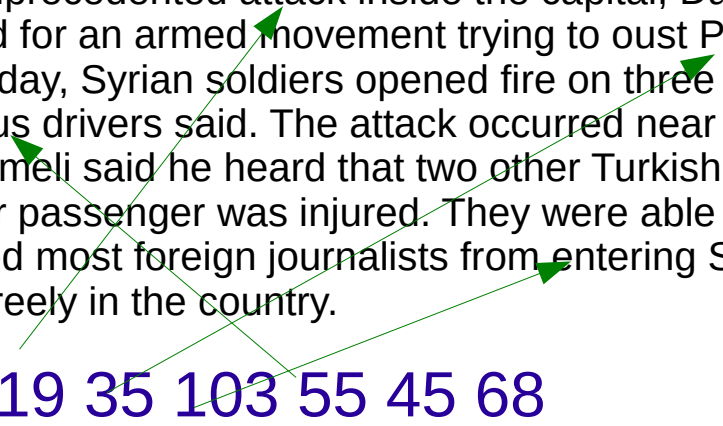
The commander of a group of Syrian army defectors retracted earlier claims that his followers launched an unprecedented attack inside the capital, Damascus, in an embarrassing turnaround for an armed movement trying to oust President Bashar Assad’s regime. lso Monday, Syrian soldiers opened fire on three Turkish buses, injuring two people, one of the bus drivers said. The attack occurred near the central city of Homs early Monday. Surmeli said he heard that two other Turkish buses had come under attack and another passenger was injured. They were able to cross into Turkey, he said. Syria has banned most foreign journalists from entering Syria and prevented the media from moving freely in the country.

19 35 103 55 45 68

This is only for example to show the seriousness. Author is not responsible for any future usage.

The Intuition

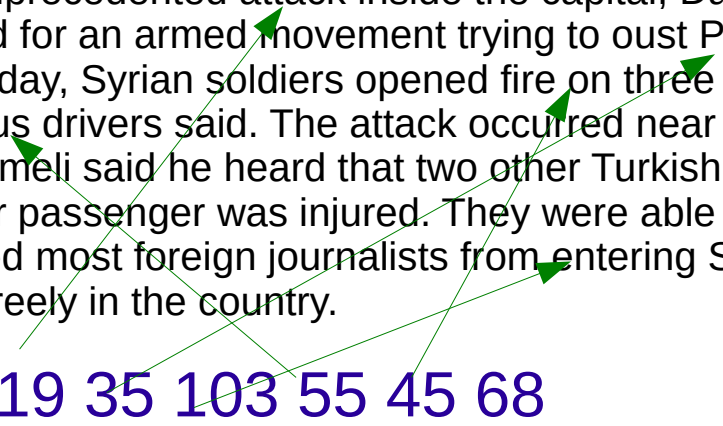
The commander of a group of Syrian army defectors retracted earlier claims that his followers launched an unprecedented attack inside the capital, Damascus, in an embarrassing turnaround for an armed movement trying to oust President Bashar Assad’s regime. lso Monday, Syrian soldiers opened fire on three Turkish buses, injuring two people, one of the bus drivers said. The attack occurred near the central city of Homs early Monday. Surmeli said he heard that two other Turkish buses had come under attack and another passenger was injured. They were able to cross into Turkey, he said. Syria has banned most foreign journalists from entering Syria and prevented the media from moving freely in the country.



This is only for example to show the seriousness. Author is not responsible for any future usage.

The Intuition

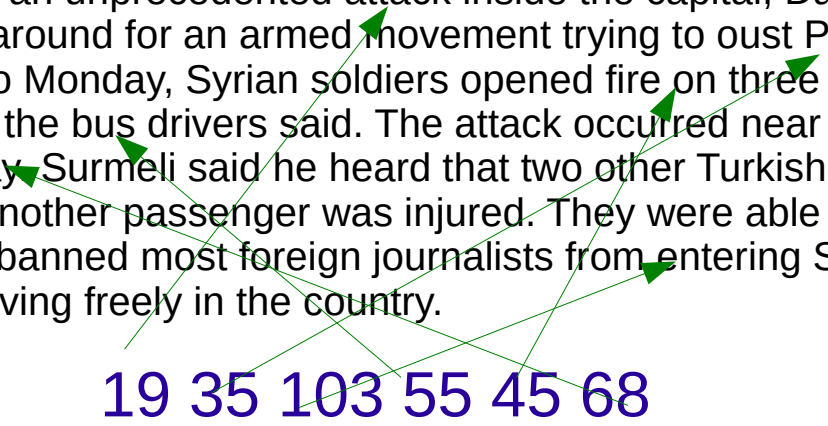
The commander of a group of Syrian army defectors retracted earlier claims that his followers launched an unprecedented attack inside the capital, Damascus, in an embarrassing turnaround for an armed movement trying to oust President Bashar Assad’s regime. lso Monday, Syrian soldiers opened fire on three Turkish buses, injuring two people, one of the bus drivers said. The attack occurred near the central city of Homs early Monday. Surmeli said he heard that two other Turkish buses had come under attack and another passenger was injured. They were able to cross into Turkey, he said. Syria has banned most foreign journalists from entering Syria and prevented the media from moving freely in the country.



This is only for example to show the seriousness. Author is not responsible for any future usage.

The Intuition

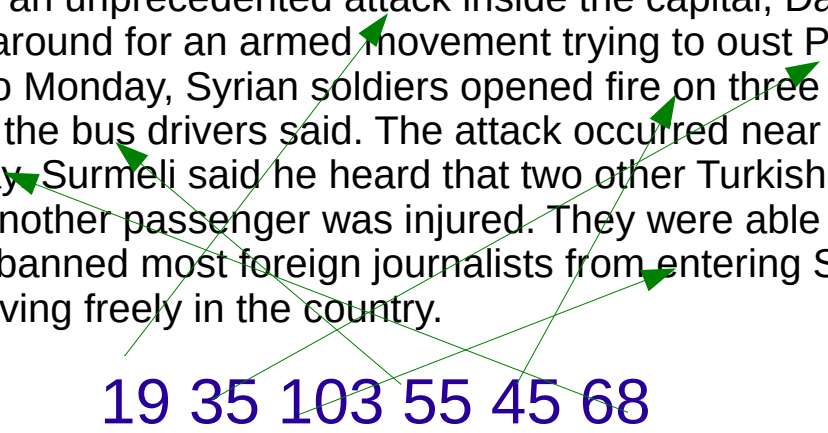
The commander of a group of Syrian army defectors retracted earlier claims that his followers launched an unprecedented attack inside the capital, Damascus, in an embarrassing turnaround for an armed movement trying to oust President Bashar Assad’s regime. lso Monday, Syrian soldiers opened fire on three Turkish buses, injuring two people, one of the bus drivers said. The attack occurred near the central city of Homs early Monday. Surmeli said he heard that two other Turkish buses had come under attack and another passenger was injured. They were able to cross into Turkey, he said. Syria has banned most foreign journalists from entering Syria and prevented the media from moving freely in the country.



This is only for example to show the seriousness. Author is not responsible for any future usage.

The Intuition

The commander of a group of Syrian army defectors retracted earlier claims that his followers launched an unprecedented attack inside the capital, Damascus, in an embarrassing turnaround for an armed movement trying to oust President Bashar Assad's regime. lso Monday, Syrian soldiers opened fire on three Turkish buses, injuring two people, one of the bus drivers said. The attack occurred near the central city of Homs early Monday. Surmeli said he heard that two other Turkish buses had come under attack and another passenger was injured. They were able to cross into Turkey, he said. Syria has banned most foreign journalists from entering Syria and prevented the media from moving freely in the country.



19 35 103 55 45 68

"Attack President entering bus on monday#"

This is only for example to show the seriousness. Author is not responsible for any future usage.

Extending to computers → ROP

Extending to computers → ROP

- Newspaper → available memory

Extending to computers → ROP

- Newspaper → available memory
- Words → instructions

Extending to computers → ROP

- Newspaper → available memory
- Words → instructions
- Space → Return

Extending to computers → ROP

- Newspaper → available memory
- Words → instructions
- Space → Return
- Offset → EIP

Extending to computers → ROP

- Newspaper → available memory
- Words → instructions
- Space → Return
- Offset → EIP
- Message → shellcode

Extending to computers → ROP

- Newspaper → available memory
- Words → instructions
- Space → Return
- Offset → EIP
- Message → shellcode

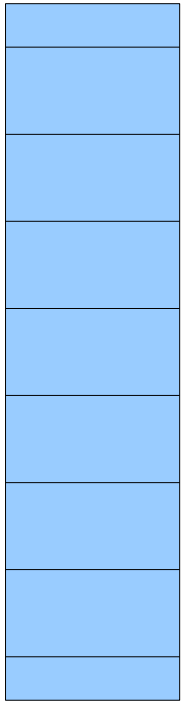
And we get....

Conti...

Memory

The commander of a group of Syrian army defectors retracted earlier claims that his followers launched an unprecedented attack inside the capital, Damascus, in an embarrassing turnaround for an armed movement trying to oust President Bashar Assad's regime. lso Monday, Syrian soldiers opened fire on three Turkish buses, injuring two people, one of the bus drivers said. The attack occurred near the central city of Homs early Monday. Surmeli said he heard that two other Turkish buses had come under attack and another passenger was injured. They were able to cross into Turkey, he said. Syria has banned most foreign journalists from entering Syria and prevented the media from moving freely in the country.

Stack

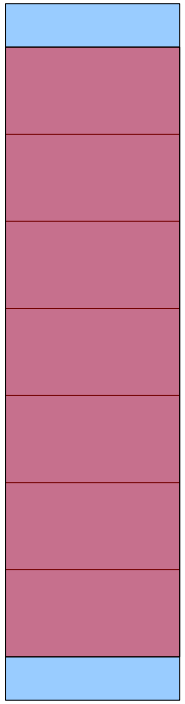


Conti...

Memory

The commander of a group of Syrian army defectors retracted earlier claims that his followers launched an unprecedented attack inside the capital, Damascus, in an embarrassing turnaround for an armed movement trying to oust President Bashar Assad's regime. lso Monday, Syrian soldiers opened fire on three Turkish buses, injuring two people, one of the bus drivers said. The attack occurred near the central city of Homs early Monday. Surmeli said he heard that two other Turkish buses had come under attack and another passenger was injured. They were able to cross into Turkey, he said. Syria has banned most foreign journalists from entering Syria and prevented the media from moving freely in the country.

Stack

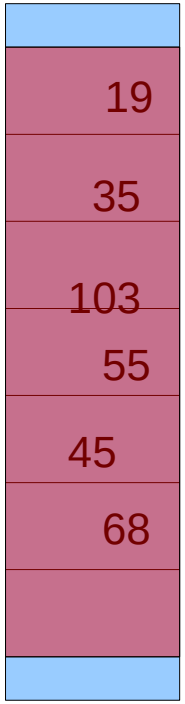


Conti...

Memory

The commander of a group of Syrian army defectors retracted earlier claims that his followers launched an unprecedented attack inside the capital, Damascus, in an embarrassing turnaround for an armed movement trying to oust President Bashar Assad's regime. lso Monday, Syrian soldiers opened fire on three Turkish buses, injuring two people, one of the bus drivers said. The attack occurred near the central city of Homs early Monday. Surmeli said he heard that two other Turkish buses had come under attack and another passenger was injured. They were able to cross into Turkey, he said. Syria has banned most foreign journalists from entering Syria and prevented the media from moving freely in the country.

Stack

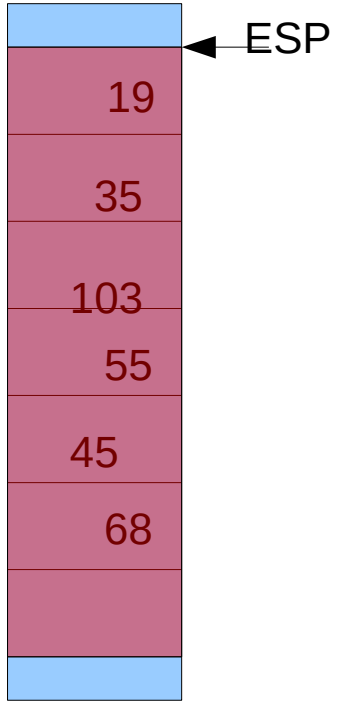


Conti...

Memory

The commander of a group of Syrian army defectors retracted earlier claims that his followers launched an unprecedented attack inside the capital, Damascus, in an embarrassing turnaround for an armed movement trying to oust President Bashar Assad's regime. lso Monday, Syrian soldiers opened fire on three Turkish buses, injuring two people, one of the bus drivers said. The attack occurred near the central city of Homs early Monday. Surmeli said he heard that two other Turkish buses had come under attack and another passenger was injured. They were able to cross into Turkey, he said. Syria has banned most foreign journalists from entering Syria and prevented the media from moving freely in the country.

Stack



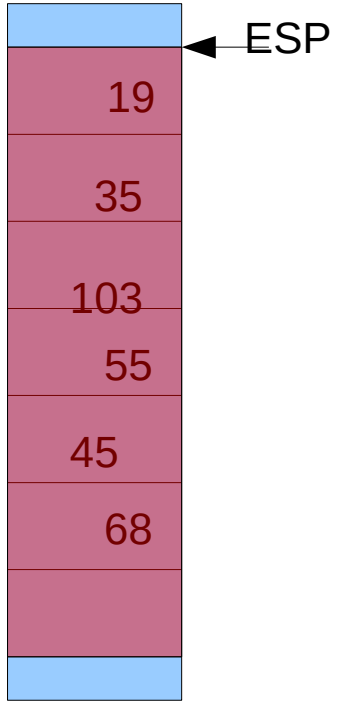
Conti...

Memory

The commander of a group of Syrian army defectors retracted earlier claims that his followers launched an unprecedented attack inside the capital, Damascus, in an embarrassing turnaround for an armed movement trying to oust President Bashar Assad's regime. lso Monday, Syrian soldiers opened fire on three Turkish buses, injuring two people, one of the bus drivers said. The attack occurred near the central city of Homs early Monday. Surmeli said he heard that two other Turkish buses had come under attack and another passenger was injured. They were able to cross into Turkey, he said. Syria has banned most foreign journalists from entering Syria and prevented the media from moving freely in the country.

RET

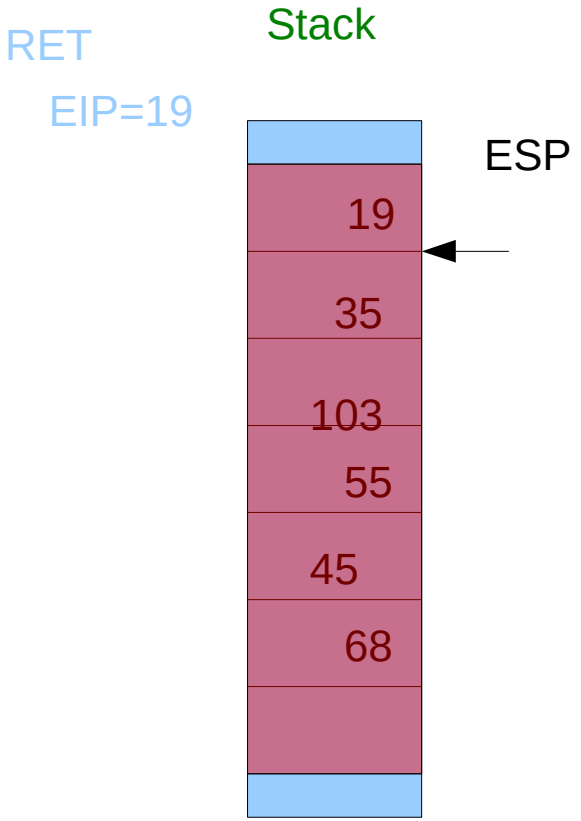
Stack



Conti...

Memory

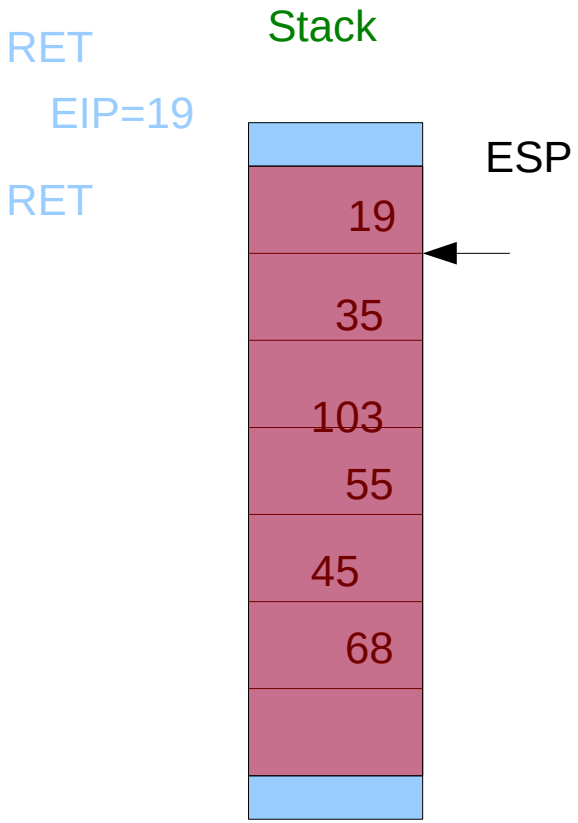
The commander of a group of Syrian army defectors retracted earlier claims that his followers launched an unprecedented attack inside the capital, Damascus, in an embarrassing turnaround for an armed movement trying to oust President Bashar Assad's regime. lso Monday, Syrian soldiers opened fire on three Turkish buses, injuring two people, one of the bus drivers said. The attack occurred near the central city of Homs early Monday. Surmeli said he heard that two other Turkish buses had come under attack and another passenger was injured. They were able to cross into Turkey, he said. Syria has banned most foreign journalists from entering Syria and prevented the media from moving freely in the country.



Conti...

Memory

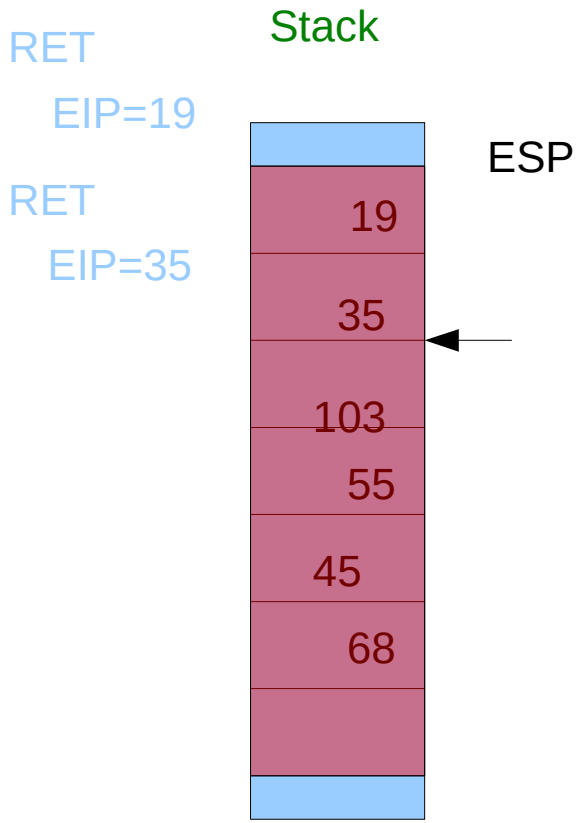
The commander of a group of Syrian army defectors retracted earlier claims that his followers launched an unprecedented attack inside the capital, Damascus, in an embarrassing turnaround for an armed movement trying to oust President Bashar Assad's regime. lso Monday, Syrian soldiers opened fire on three Turkish buses, injuring two people, one of the bus drivers said. The attack occurred near the central city of Homs early Monday. Surmeli said he heard that two other Turkish buses had come under attack and another passenger was injured. They were able to cross into Turkey, he said. Syria has banned most foreign journalists from entering Syria and prevented the media from moving freely in the country.



Conti...

Memory

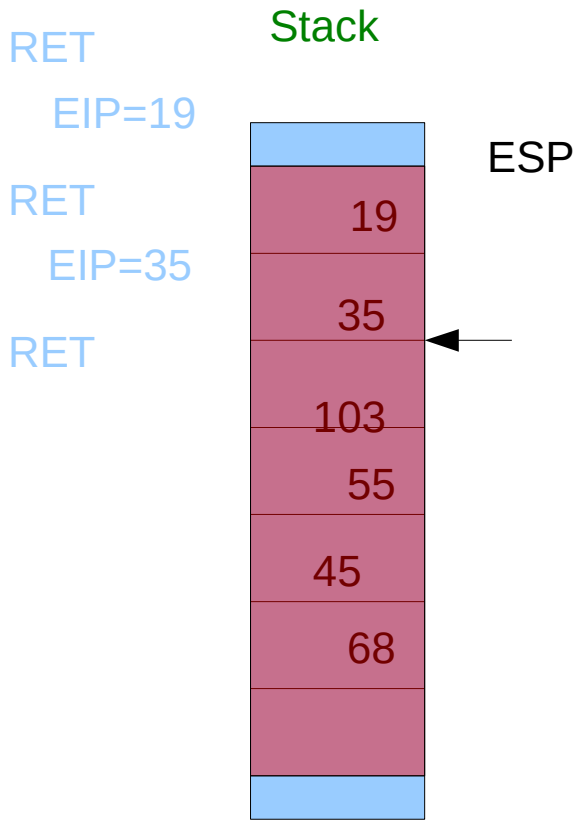
The commander of a group of Syrian army defectors retracted earlier claims that his followers launched an unprecedented attack inside the capital, Damascus, in an embarrassing turnaround for an armed movement trying to oust President Bashar Assad's regime. lso Monday, Syrian soldiers opened fire on three Turkish buses, injuring two people, one of the bus drivers said. The attack occurred near the central city of Homs early Monday. Surmeli said he heard that two other Turkish buses had come under attack and another passenger was injured. They were able to cross into Turkey, he said. Syria has banned most foreign journalists from entering Syria and prevented the media from moving freely in the country.



Conti...

Memory

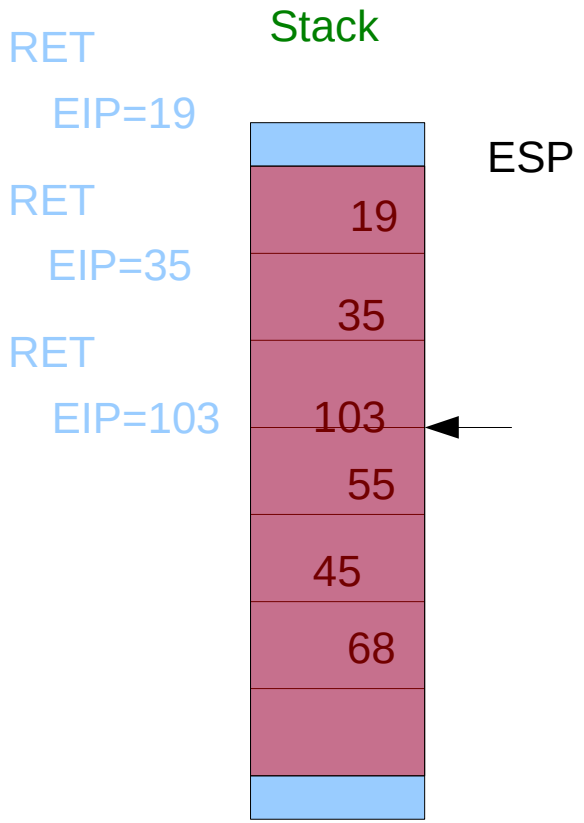
The commander of a group of Syrian army defectors retracted earlier claims that his followers launched an unprecedented attack inside the capital, Damascus, in an embarrassing turnaround for an armed movement trying to oust President Bashar Assad's regime. lso Monday, Syrian soldiers opened fire on three Turkish buses, injuring two people, one of the bus drivers said. The attack occurred near the central city of Homs early Monday. Surmeli said he heard that two other Turkish buses had come under attack and another passenger was injured. They were able to cross into Turkey, he said. Syria has banned most foreign journalists from entering Syria and prevented the media from moving freely in the country.



Conti...

Memory

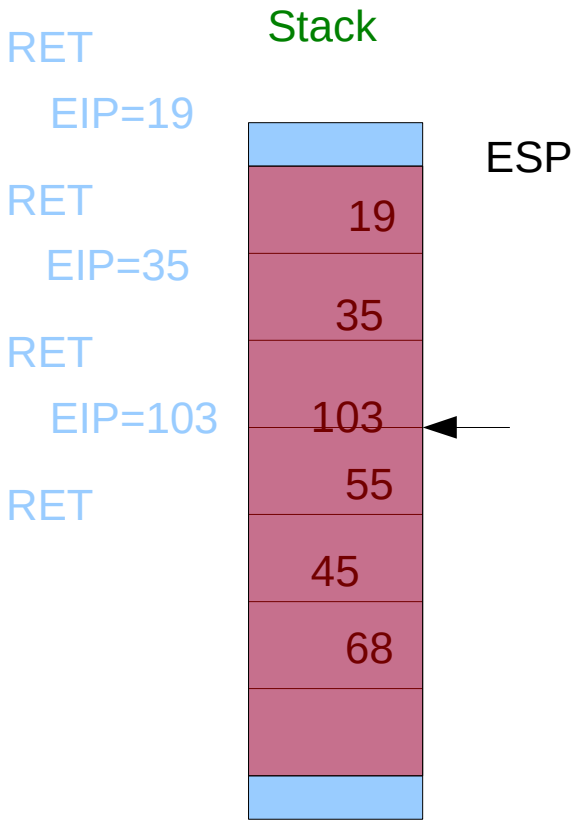
The commander of a group of Syrian army defectors retracted earlier claims that his followers launched an unprecedented attack inside the capital, Damascus, in an embarrassing turnaround for an armed movement trying to oust President Bashar Assad's regime. lso Monday, Syrian soldiers opened fire on three Turkish buses, injuring two people, one of the bus drivers said. The attack occurred near the central city of Homs early Monday. Surmeli said he heard that two other Turkish buses had come under attack and another passenger was injured. They were able to cross into Turkey, he said. Syria has banned most foreign journalists from entering Syria and prevented the media from moving freely in the country.



Conti...

Memory

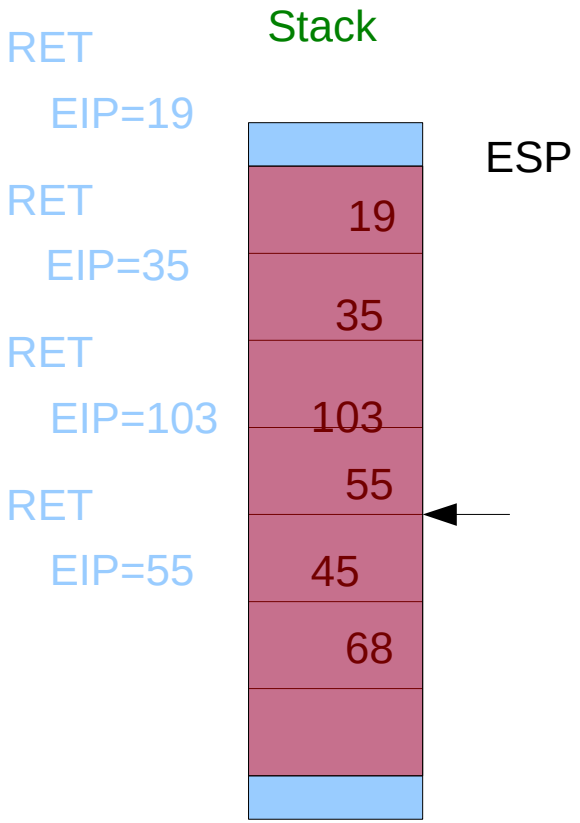
The commander of a group of Syrian army defectors retracted earlier claims that his followers launched an unprecedented attack inside the capital, Damascus, in an embarrassing turnaround for an armed movement trying to oust President Bashar Assad's regime. lso Monday, Syrian soldiers opened fire on three Turkish buses, injuring two people, one of the bus drivers said. The attack occurred near the central city of Homs early Monday. Surmeli said he heard that two other Turkish buses had come under attack and another passenger was injured. They were able to cross into Turkey, he said. Syria has banned most foreign journalists from entering Syria and prevented the media from moving freely in the country.



Conti...

Memory

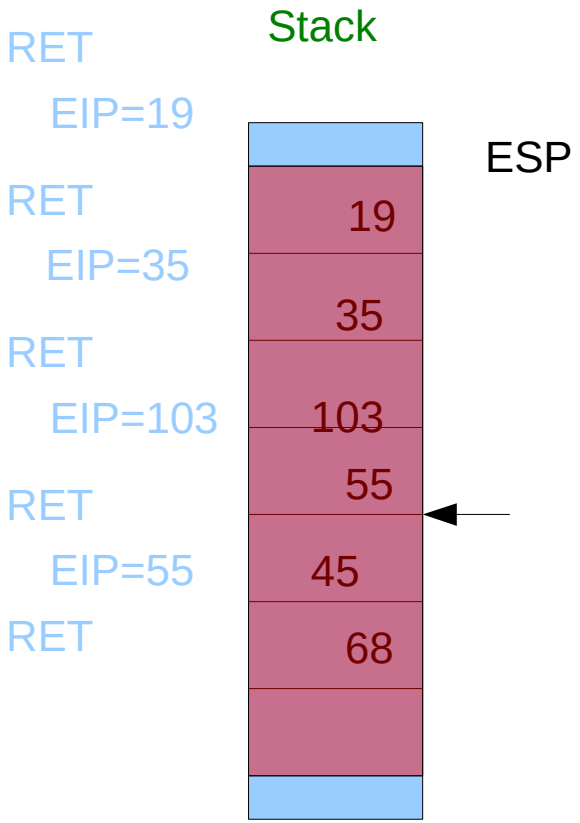
The commander of a group of Syrian army defectors retracted earlier claims that his followers launched an unprecedented attack inside the capital, Damascus, in an embarrassing turnaround for an armed movement trying to oust President Bashar Assad's regime. Iso Monday, Syrian soldiers opened fire on three Turkish buses, injuring two people, one of the bus drivers said. The attack occurred near the central city of Homs early Monday. Surmeli said he heard that two other Turkish buses had come under attack and another passenger was injured. They were able to cross into Turkey, he said. Syria has banned most foreign journalists from entering Syria and prevented the media from moving freely in the country.



Conti...

Memory

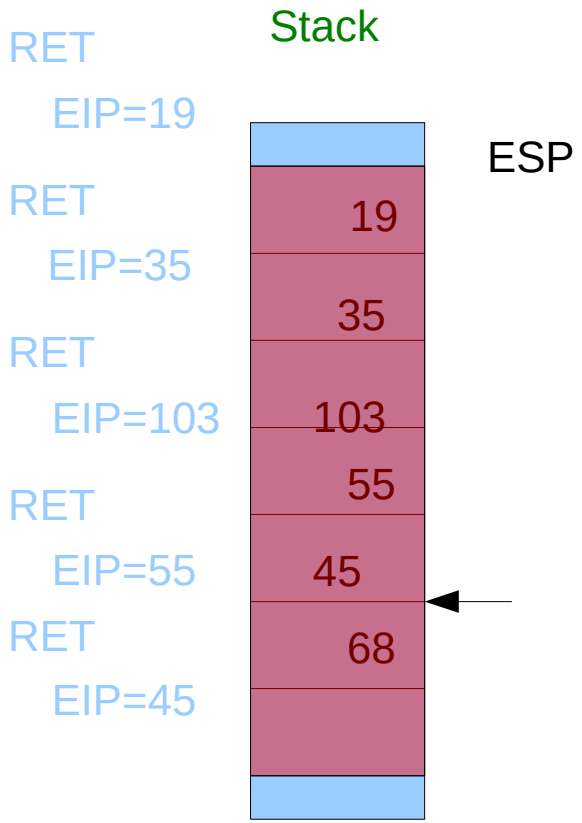
The commander of a group of Syrian army defectors retracted earlier claims that his followers launched an unprecedented attack inside the capital, Damascus, in an embarrassing turnaround for an armed movement trying to oust President Bashar Assad's regime. Iso Monday, Syrian soldiers opened fire on three Turkish buses, injuring two people, one of the bus drivers said. The attack occurred near the central city of Homs early Monday. Surmeli said he heard that two other Turkish buses had come under attack and another passenger was injured. They were able to cross into Turkey, he said. Syria has banned most foreign journalists from entering Syria and prevented the media from moving freely in the country.



Conti...

Memory

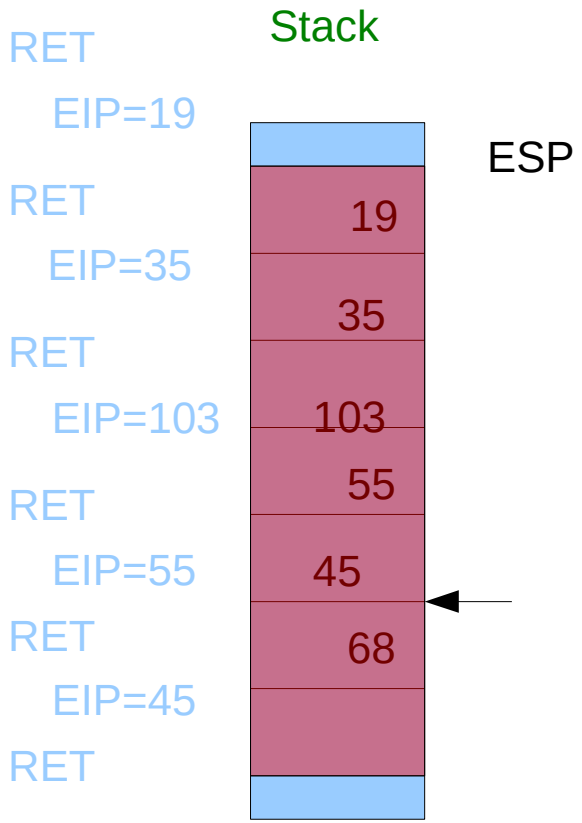
The commander of a group of Syrian army defectors retracted earlier claims that his followers launched an unprecedented attack inside the capital, Damascus, in an embarrassing turnaround for an armed movement trying to oust President Bashar Assad's regime. Iso Monday, Syrian soldiers opened fire on three Turkish buses, injuring two people, one of the bus drivers said. The attack occurred near the central city of Homs early Monday. Surmeli said he heard that two other Turkish buses had come under attack and another passenger was injured. They were able to cross into Turkey, he said. Syria has banned most foreign journalists from entering Syria and prevented the media from moving freely in the country.



Conti...

Memory

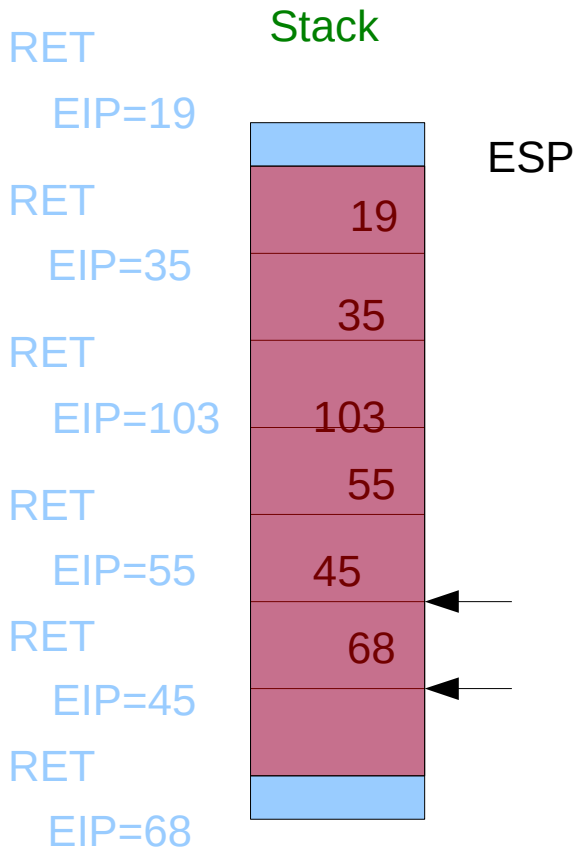
The commander of a group of Syrian army defectors retracted earlier claims that his followers launched an unprecedented attack inside the capital, Damascus, in an embarrassing turnaround for an armed movement trying to oust President Bashar Assad's regime. Iso Monday, Syrian soldiers opened fire on three Turkish buses, injuring two people, one of the bus drivers said. The attack occurred near the central city of Homs early Monday. Surmeli said he heard that two other Turkish buses had come under attack and another passenger was injured. They were able to cross into Turkey, he said. Syria has banned most foreign journalists from entering Syria and prevented the media from moving freely in the country.



Conti...

Memory

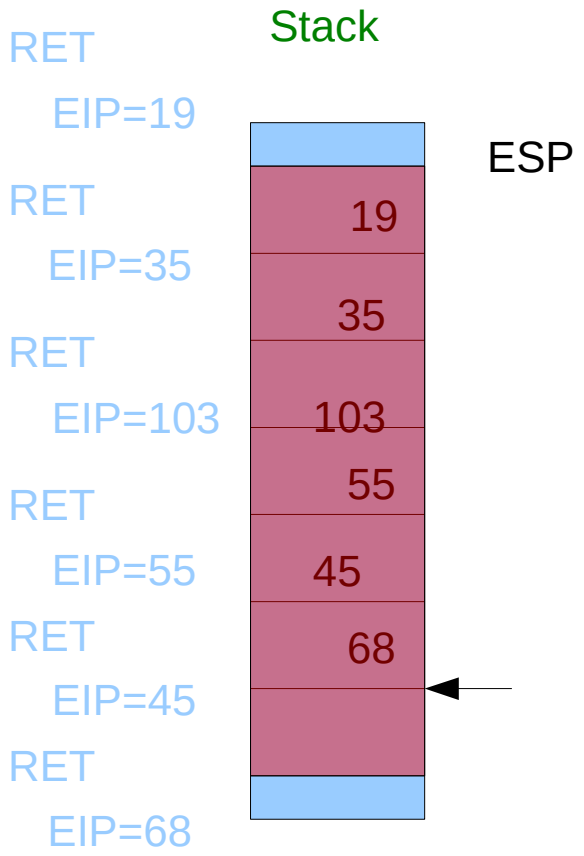
The commander of a group of Syrian army defectors retracted earlier claims that his followers launched an unprecedented attack inside the capital, Damascus, in an embarrassing turnaround for an armed movement trying to oust President Bashar Assad's regime. Iso Monday, Syrian soldiers opened fire on three Turkish buses, injuring two people, one of the bus drivers said. The attack occurred near the central city of Homs early Monday. Surmeli said he heard that two other Turkish buses had come under attack and another passenger was injured. They were able to cross into Turkey, he said. Syria has banned most foreign journalists from entering Syria and prevented the media from moving freely in the country.



Conti...

Memory

The commander of a group of Syrian army defectors retracted earlier claims that his followers launched an unprecedented attack inside the capital, Damascus, in an embarrassing turnaround for an armed movement trying to oust President Bashar Assad's regime. lso Monday, Syrian soldiers opened fire on three Turkish buses, injuring two people, one of the bus drivers said. The attack occurred near the central city of Homs early Monday. Surmeli said he heard that two other Turkish buses had come under attack and another passenger was injured. They were able to cross into Turkey, he said. Syria has banned most foreign journalists from entering Syria and prevented the media from moving freely in the country.



An Example

- "*How to make backdoor with Return Oriented Programming & ROPgadget tool*" (Jonathan Salwan) @Shell-Storm.org
- Executables have code and data for computing
  - We need to supply necessary data
  - ROP is for code part.

A Vulnerable Program

```
int copyData(char *string)
{
    char buf[32];
    strcpy(buf, string);
    return (0);
}

int main()
{
    char buffer[700];
    FILE *file;
    printf("opening file");
    file = fopen("exploitFile","rb");
    if (!file)
    {
        fprintf(stderr,"file not opened %s",
strerror(errno));
        return (0);
    }
    printf("file opened");
    fread(buffer, 699,1,file);
    fclose(file);
    copyData(buffer);
    return (0);
}
```

What We Want to Get...

What We Want to Get...

We want to get a shell… (as usual!)

What We Want to Get...

We want to get a shell… (as usual!)

```
int main()
{
      char *env[1] = {NULL};
      char *arguments[3]= { "/bin//sh",
                NULL
               };
      execve("/bin//sh", arguments, env);
}
```

What We Want to Get...

We want to get a shell… (as usual!)

```
int main()
{
      char *env[1] = {NULL};
      char *arguments[3]= { "/bin//sh",
                NULL
               };
      execve("/bin//sh", arguments, env);
}
```

We use INT80 instruction →

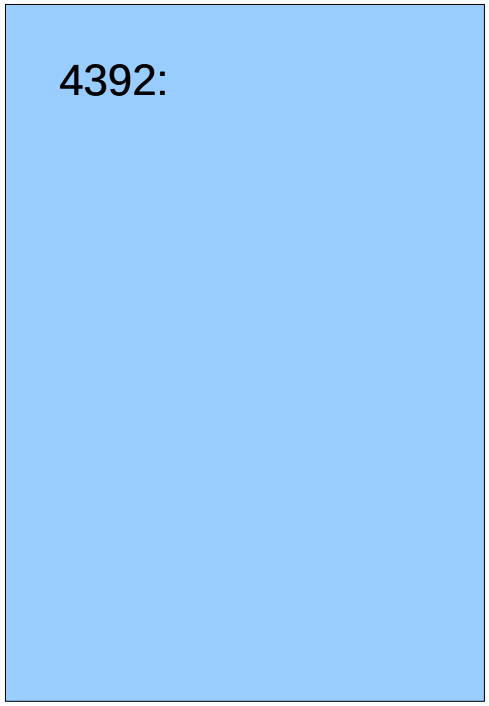
EAX = 11
EBX = "/bin//sh" (char *)
ECX = arguments (char **)
EDX = env (char **) (NULL)
ESI =...., EDI = ...

Execution Plan

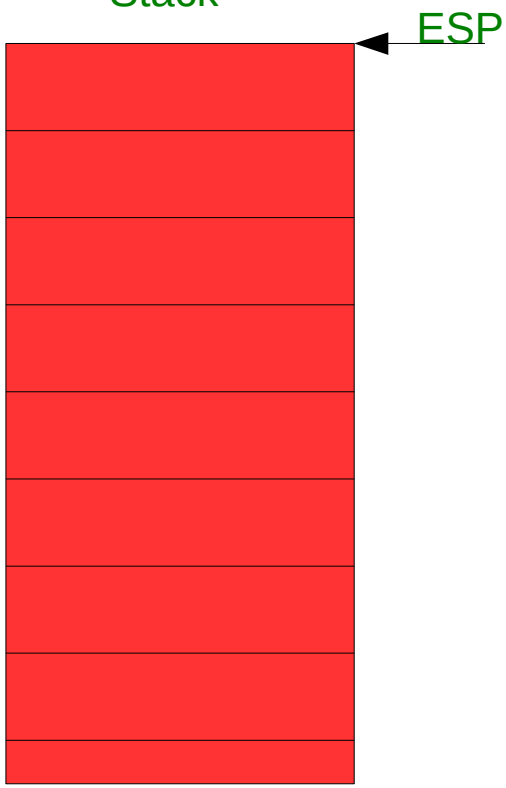
- Find a place in the executable to store data (dummy-stack)
- Use objdump utility for .data section
- Select a region, initialized with zeros
- Find gadgets to POP data from stack and MOV that to dummy-stack
- Find gadgets to INC EAX (syscall number)

Preparing Data

Data section



Stack



Preparing Data

Preparing Data

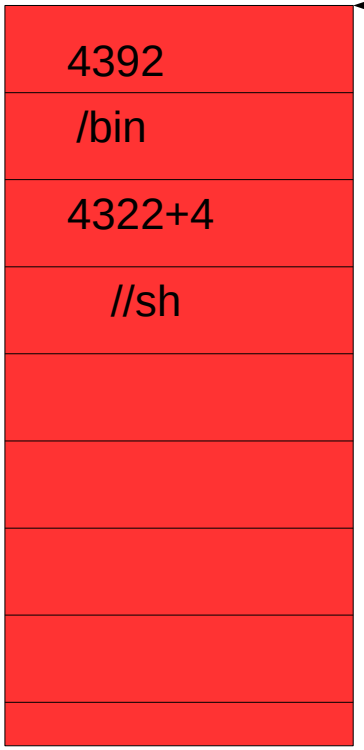
Data section

4392:

POP ecx ret

Stack

ESP



Preparing Data

Data section

4392:

POP ecx ret

ecx=4392

Stack

ESP

Preparing Data

Data section

4392:

POP ecx ret

POP eax ret

ecx=4392

Stack

ESP

Preparing Data

Data section

4392:

POP ecx ret

POP eax ret

ecx=4392

eax=/bin

Stack

ESP

Preparing Data

Data section

4392:

POP ecx ret

POP eax ret

MOV [ecx] eax ret

ecx=4392

eax=/bin

Stack

ESP

Preparing Data

Data section

4392: /bin

POP ecx ret

POP eax ret

MOV [ecx] eax ret

ecx=4392

eax=/bin

Stack

ESP

Preparing Data

Data section

4392: /bin

POP ecx ret

POP eax ret

MOV [ecx] eax ret

POP ecx ret

ecx=4392

eax=/bin

Stack

ESP

Preparing Data

Data section

4392: /bin

4396:

POP ecx ret

POP eax ret

MOV [ecx] eax ret

POP ecx ret

ecx=4392

eax=/bin

ecx=4396

Stack

ESP

Preparing Data

Data section

4392: /bin

4396:

POP ecx ret

POP eax ret

MOV [ecx] eax ret

POP ecx ret

POP eax ret

ecx=4392

eax=/bin

ecx=4396

Stack

ESP

Preparing Data

Data section

4392: /bin

4396:

POP ecx ret

POP eax ret

MOV [ecx] eax ret

POP ecx ret

POP eax ret

ecx=4392

eax=/bin

ecx=4396

eax=//sh

Stack

ESP

Preparing Data

Data section

4392: /bin

4396:

POP ecx ret

POP eax ret

ecx=4392

eax=/bin

MOV [ecx] eax ret

POP ecx ret

POP eax ret

ecx=4396

eax=//sh

MOV [ecx] eax ret

Stack

ESP

Preparing Data

Data section

4392: /bin

4396: //sh

POP ecx ret

POP eax ret

ecx=4392

eax=/bin

MOV [ecx] eax ret

POP ecx ret

POP eax ret

ecx=4396

eax=//sh

MOV [ecx] eax ret

Stack

ESP

Preparing Data

Data section

4392: /bin

4396: //sh

POP ecx ret

POP eax ret

ecx=4392

eax=/bin

MOV [ecx] eax ret

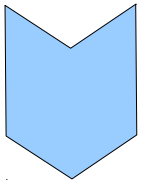
POP ecx ret

POP eax ret

ecx=4396

eax=//sh

MOV [ecx] eax ret



Stack

ESP

Preparing Data

Data section

4392: /bin

4396: //sh

POP ecx ret

POP eax ret

MOV [ecx] eax ret

POP ecx ret

POP eax ret

MOV [ecx] eax ret

ecx=4392

eax=/bin

ecx=4396

eax=//sh

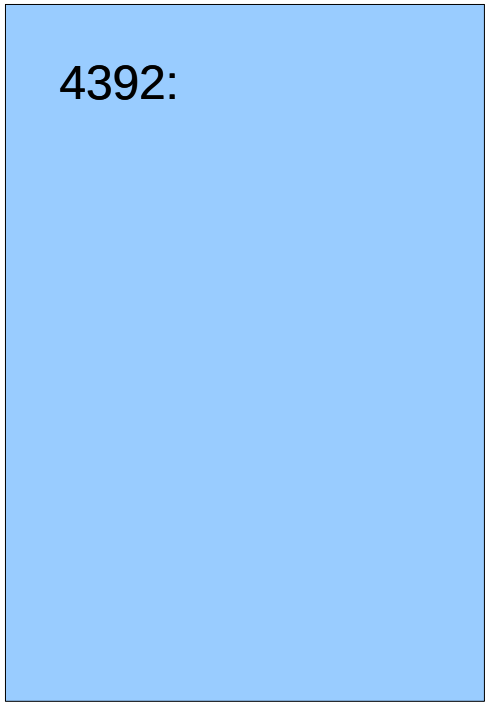
Stack

ESP

ROP Gadget

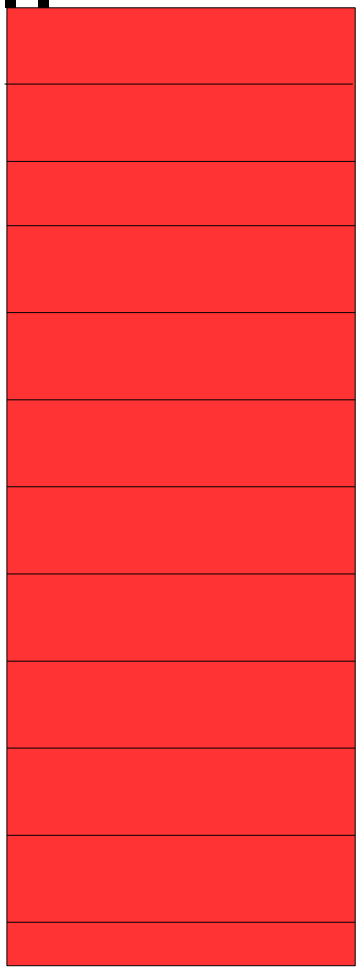
Preparing Data II

Data section



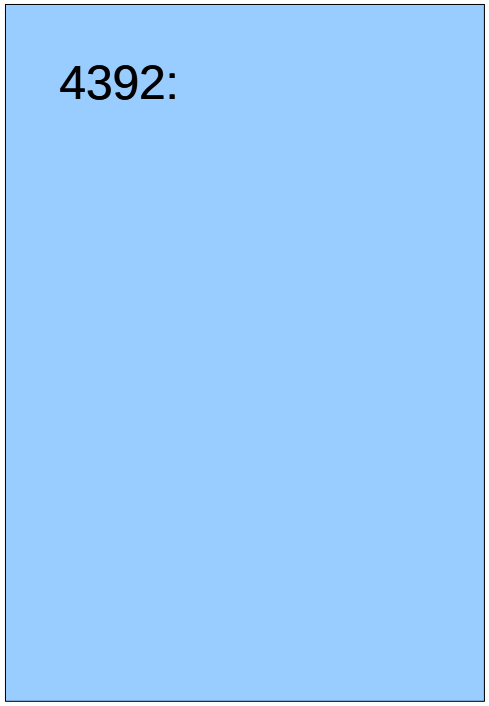
Stack

ESP



Preparing Data II

Data section



Stack

ESP

Preparing Data II

Data section

4392:

POP ecx ret

Stack

ESP

Preparing Data II

Data section

4392:

POP ecx ret

ecx=4392

Stack

ESP

Preparing Data II

Data section

4392:

POP ecx ret

POP eax ret

ecx=4392

Stack

ESP

Preparing Data II

Data section

4392:

POP ecx ret

POP eax ret

ecx=4392

eax=/bin

Stack

ESP

Preparing Data II

Data section

4392:

POP ecx ret

POP eax ret

ecx=4392

eax=/bin

MOV [ecx] eax ret

Stack

ESP

Preparing Data II

Data section

4392: /bin

POP ecx ret

POP eax ret

ecx=4392

eax=/bin

MOV [ecx] eax ret

Stack

ESP

Preparing Data II

Data section

4392: /bin

POP ecx ret

POP eax ret

ecx=4392

eax=/bin

MOV [ecx] eax ret

POP ecx ret

Stack

ESP

Preparing Data II

Data section

4392: /bin

4396:

POP ecx ret

POP eax ret

ecx=4392

eax=/bin

MOV [ecx] eax ret

POP ecx ret

ecx=4396

Stack

ESP

Preparing Data II

Data section

4392: /bin

4396:

POP ecx ret

POP eax ret

ecx=4392

eax=/bin

MOV [ecx] eax ret

POP ecx ret

POP eax ret

ecx=4396

Preparing Data II

Data section

4392: /bin

4396:

POP ecx ret

POP eax ret

ecx=4392

eax=/bin

MOV [ecx] eax ret

POP ecx ret

POP eax ret

ecx=4396

eax=//sh

Preparing Data II

Data section

4392: /bin

4396: //sh

POP ecx ret

POP eax ret

ecx=4392

eax=/bin

MOV [ecx] eax ret

POP ecx ret

POP eax ret

ecx=4396

eax=//sh

Stack

ESP

Preparing Data II

Data section

4392: /bin

4396: //sh

POP ecx ret

POP eax ret

ecx=4392

eax=/bin

MOV [ecx] eax ret

POP ecx ret

POP eax ret

ecx=4396

eax=//sh

Stack

ESP

And process is repeated.....

The real code

- Lets look at the real python code

Few References

- http://research.shell-storm.org/
- Ryan Roemer and Erik Buchanan and Hovav Shacham and Stefan Savage (2011), “Return-Oriented Programming: Systems, Languages, and Applications” In: Trans. Info. \& Sys. Sec.
- H. Shacham. “The Geometry of Innocent Flesh on the Bone: Return-into-libc without Function Calls (on the x86).” In S. De Capitani Di Vimercati and P. Syverson, eds., Proceedings of CCS 2007, pages 552–561. ACM Press, Oct. 2007
- Kaan Onarlioglu, Leyla Bilge, Andrea Lanzi, Davide Balzarotti, and Engin Kirda. 2010. G-Free: defeating return-oriented programming through gadget-less binaries. In Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC '10). ACM, New York, NY, USA, 49-58

Thank You!