f5

DEFEND
THE NEW PERIMETER

PyMultitor

Bypass restrictions based on IP counters like a Boss

Tomer Zait

Security Researcher, F5 Networks

DEFEND
THE NEW PERIMETER

ABOUT ME

Tomer Zait

- Security Researcher at F5
- Practical Software Engineer (Ort Singalovsky)
- Offensive Security Certified Professional (OSCP)

- LinkedIn: https://il.linkedin.com/in/realgame
- GitHub: https://github.com/realgam3

SUBJECTS

- The Problem
- About Tor
- About BruteForce
- About PyMultitor
- Can We Prevent It?

The Problem

SECTION

1

WHAT IS THE PROBLEM?

- **Security solutions that rely on IP counters**
  - Bruteforce
  - DoS
  - Anti-Scanning

About Tor

SECTION

2

ABOUT TOR

- **Tor** is a network infrastructure that allows browsing the web anonymously (This can be argued).
- The Tor network is constantly growing and includes over 4,500 servers through which one can browse the internet anonymously. In essence, this means that each server can act as an anonymous proxy with a different IP address.
- Since the Tor communication can be encrypted, it allows the communication between the end user and the proxy to be encrypted, making it harder to identify the true source.

WHAT IS TOR BROWSER?

- **The Tor Browser** was first developed and utilized by the United States Navy as an onion-routing tool to protect digital government communications
- The inventors were employees of the United States Naval Research Laboratory
- Initially designed solely for U.S. government activities, the browser is now widely used by governments around the world as well as journalists, activists, and various others

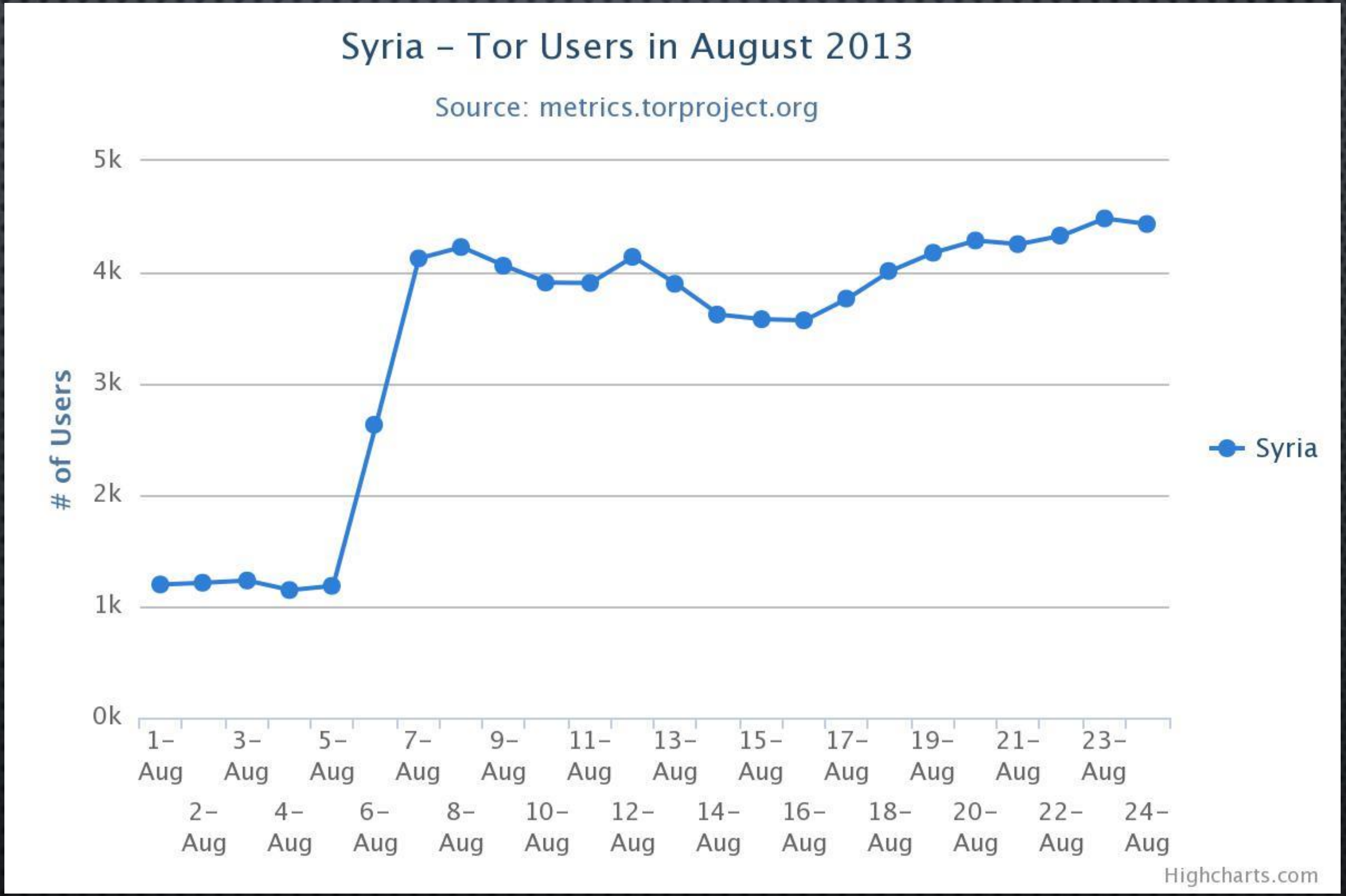
POSITIVES OF THE TOR BROWSER

- Encrypts government communications for many smaller nations
- Protects users from intrusive government surveillance
  - Used by many American citizens for simple tasks such as checking bank accounts in order to prevent network logging of information

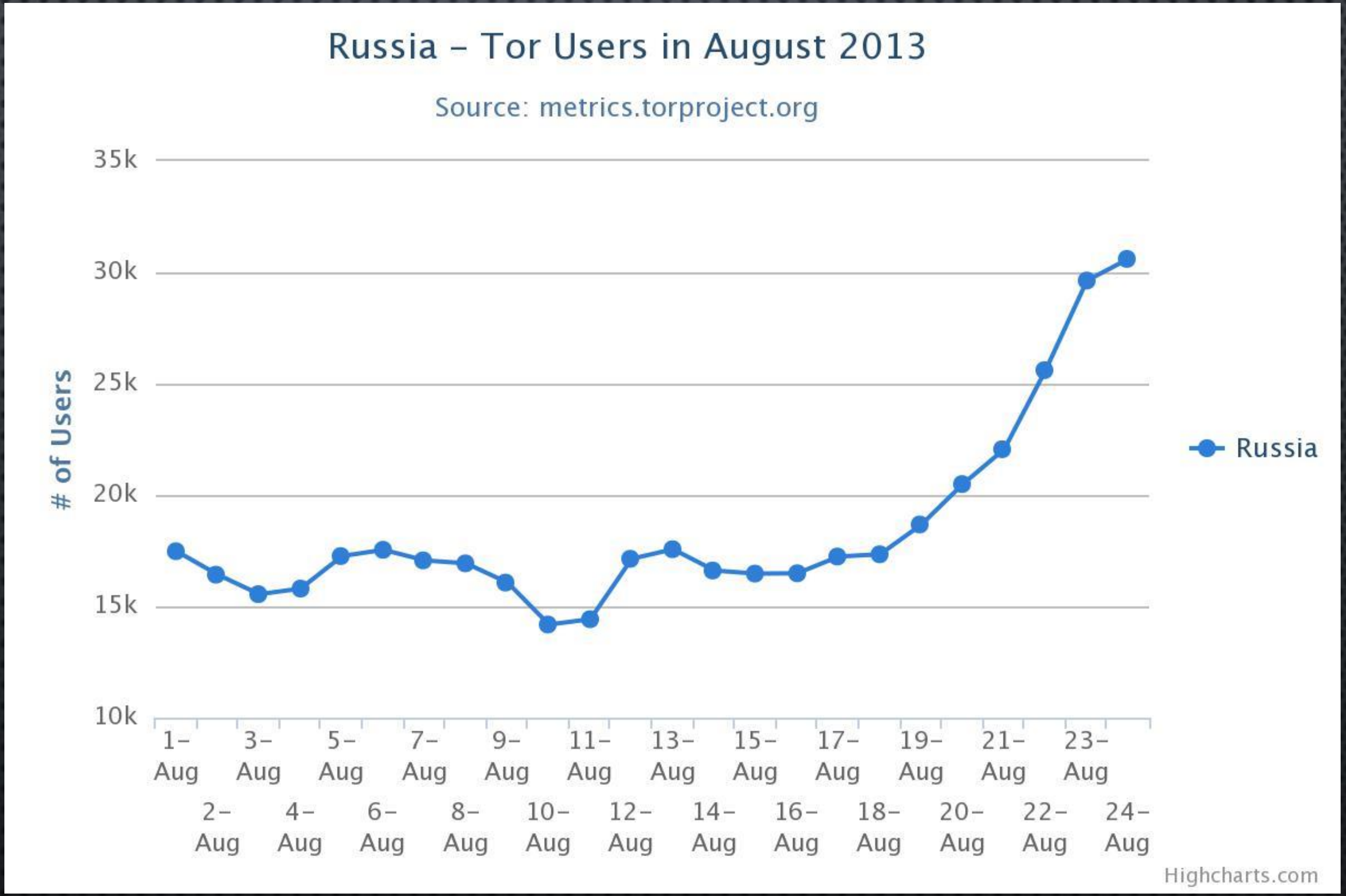
POSITIVES OF THE TOR BROWSER (1)

- Provides increased freedom for journalists in oppressed nations
- Allows individuals in nations with censorship issues to express their opinions without worry of prosecution
- In extreme censorship cases, the Tor Browser simply allows people to access everyday sites such as Facebook, Twitter, and YouTube

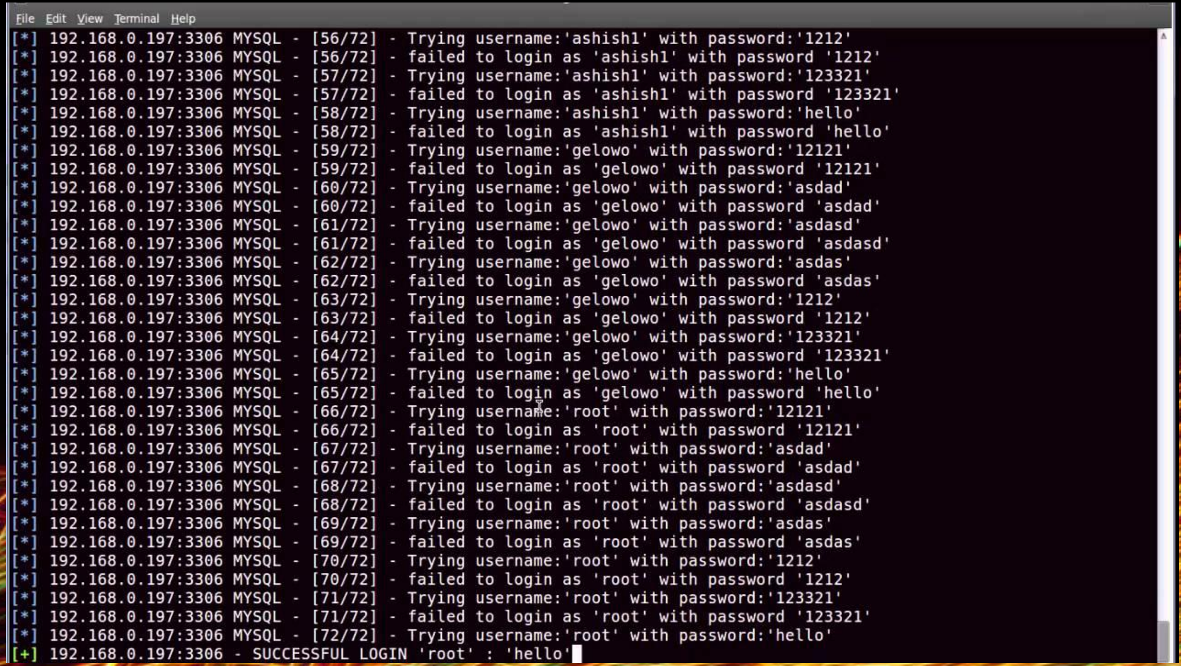
WORLDWIDE USE OF TOR



WORLDWIDE USE OF TOR (1)



About BruteForce



```
[*] 192.168.0.197:3306 MYSQL - [56/72] - Trying username:'ashish1' with password:'1212'
[*] 192.168.0.197:3306 MYSQL - [56/72] - failed to login as 'ashish1' with password '1212'
[*] 192.168.0.197:3306 MYSQL - [57/72] - Trying username:'ashish1' with password:'123321'
[*] 192.168.0.197:3306 MYSQL - [57/72] - failed to login as 'ashish1' with password '123321'
[*] 192.168.0.197:3306 MYSQL - [58/72] - Trying username:'ashish1' with password:'hello'
[*] 192.168.0.197:3306 MYSQL - [58/72] - failed to login as 'ashish1' with password 'hello'
[*] 192.168.0.197:3306 MYSQL - [59/72] - Trying username:'gelowo' with password:'12121'
[*] 192.168.0.197:3306 MYSQL - [59/72] - failed to login as 'gelowo' with password '12121'
[*] 192.168.0.197:3306 MYSQL - [60/72] - Trying username:'gelowo' with password:'asdad'
[*] 192.168.0.197:3306 MYSQL - [60/72] - failed to login as 'gelowo' with password 'asdad'
[*] 192.168.0.197:3306 MYSQL - [61/72] - Trying username:'gelowo' with password:'asdasd'
[*] 192.168.0.197:3306 MYSQL - [61/72] - failed to login as 'gelowo' with password 'asdasd'
[*] 192.168.0.197:3306 MYSQL - [62/72] - Trying username:'gelowo' with password:'asdas'
[*] 192.168.0.197:3306 MYSQL - [62/72] - failed to login as 'gelowo' with password 'asdas'
[*] 192.168.0.197:3306 MYSQL - [63/72] - Trying username:'gelowo' with password:'1212'
[*] 192.168.0.197:3306 MYSQL - [63/72] - failed to login as 'gelowo' with password '1212'
[*] 192.168.0.197:3306 MYSQL - [64/72] - Trying username:'gelowo' with password:'123321'
[*] 192.168.0.197:3306 MYSQL - [64/72] - failed to login as 'gelowo' with password '123321'
[*] 192.168.0.197:3306 MYSQL - [65/72] - Trying username:'gelowo' with password:'hello'
[*] 192.168.0.197:3306 MYSQL - [65/72] - failed to login as 'gelowo' with password 'hello'
[*] 192.168.0.197:3306 MYSQL - [66/72] - Trying username:'root' with password:'12121'
[*] 192.168.0.197:3306 MYSQL - [66/72] - failed to login as 'root' with password '12121'
[*] 192.168.0.197:3306 MYSQL - [67/72] - Trying username:'root' with password:'asdad'
[*] 192.168.0.197:3306 MYSQL - [67/72] - failed to login as 'root' with password 'asdad'
[*] 192.168.0.197:3306 MYSQL - [68/72] - Trying username:'root' with password:'asdasd'
[*] 192.168.0.197:3306 MYSQL - [68/72] - failed to login as 'root' with password 'asdasd'
[*] 192.168.0.197:3306 MYSQL - [69/72] - Trying username:'root' with password:'asdas'
[*] 192.168.0.197:3306 MYSQL - [69/72] - failed to login as 'root' with password 'asdas'
[*] 192.168.0.197:3306 MYSQL - [70/72] - Trying username:'root' with password:'1212'
[*] 192.168.0.197:3306 MYSQL - [70/72] - failed to login as 'root' with password '1212'
[*] 192.168.0.197:3306 MYSQL - [71/72] - Trying username:'root' with password:'123321'
[*] 192.168.0.197:3306 MYSQL - [71/72] - failed to login as 'root' with password '123321'
[*] 192.168.0.197:3306 MYSQL - [72/72] - Trying username:'root' with password:'hello'
[+] 192.168.0.197:3306 - SUCCESSFUL LOGIN 'root' : 'hello'
```

SECTION

3

WHAT IS BRUTEFORCE

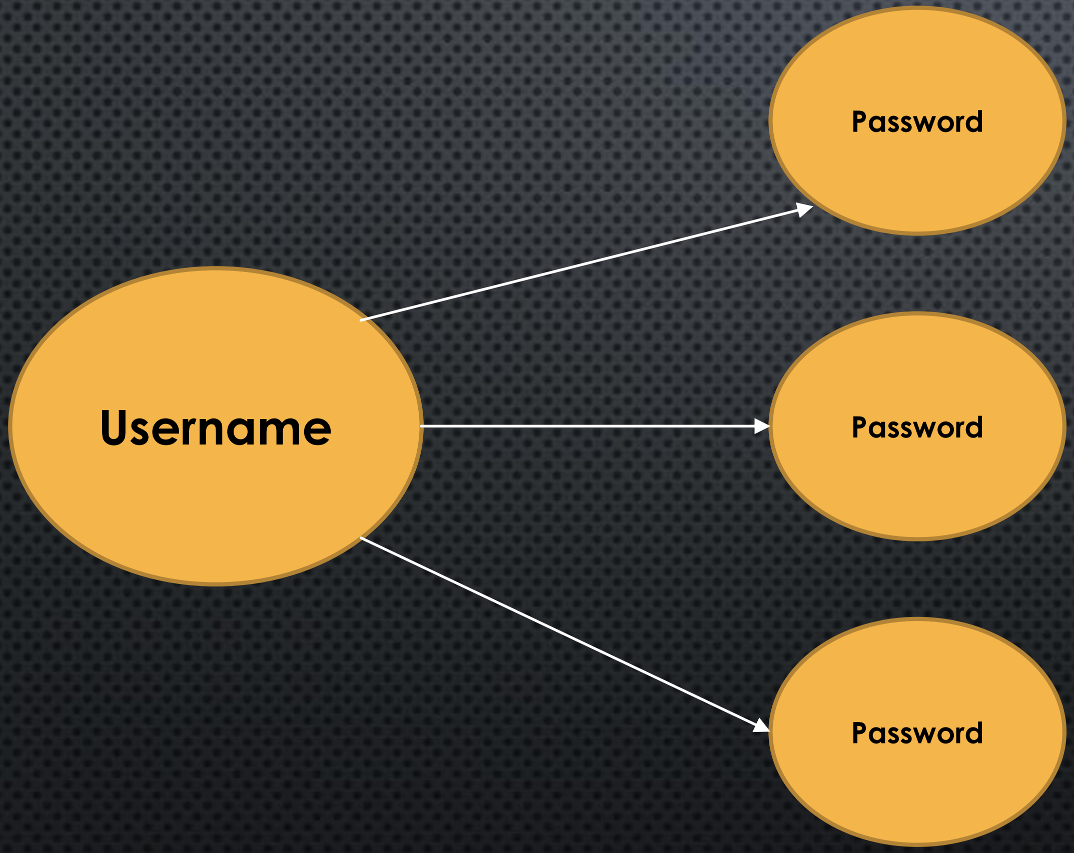
- Brute forcing consists of systematically enumerating all possible candidates for the solution and checking whether each candidate satisfies the problem's statement.
- In web application testing, the problem we are going to face with the most is very often connected with the need of having a valid user account to access the inner part of the application.
- Therefore we are going to check different types of authentication schema and the effectiveness of different brute-force attacks.

Types Of BruteForce Attacks

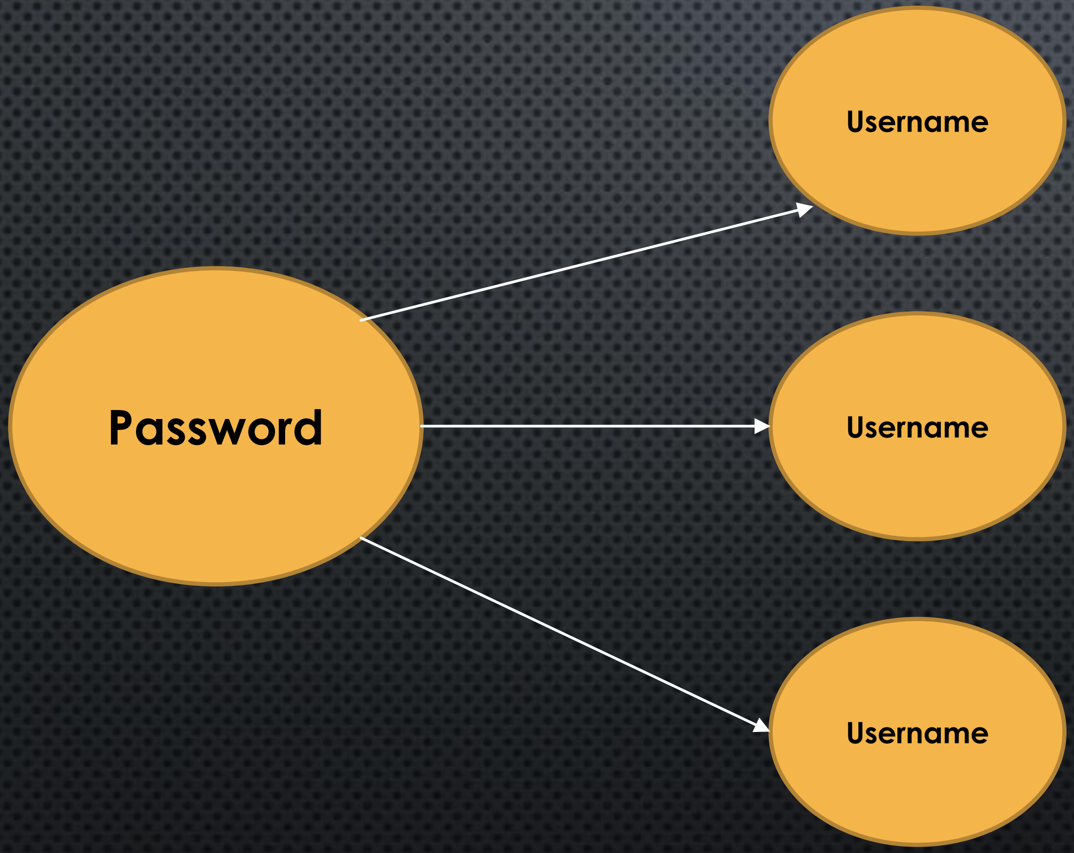
SECTION

3.1

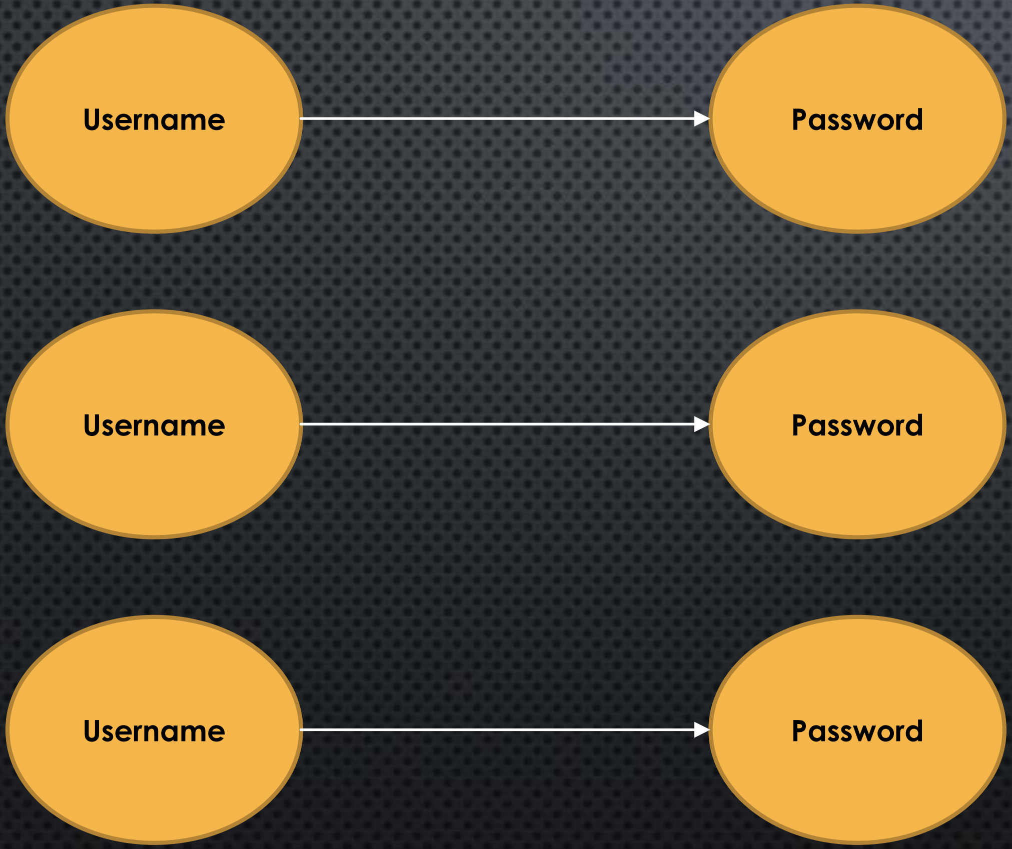
ONE USER MANY PASSWORDS



ONE PASSWORD MANY USERS



MANY USERS MANY PASSWORDS (COMBO)



About PyMultitor

SECTION

4

ABOUT THE PROJECT

Did you ever want to be at two different places at the same time?

When I asked myself this question,
I actually started developing this solution in my mind.

While performing Penetration Tests there are often problems caused by security devices that block the "attacking" IP.

ABOUT THE PROJECT (1)

This really annoyed me so I wrote a script to supply a solution for this problem.

With a large number of IP addresses performing the attacks, better results are guaranteed.

Especially when attempting attacks to bypass Web Application Firewalls, Brute-Force type attacks and many more.

WHY DID I CHOOSE TOR?

- Reliable
  - Anonymous proxies die fast and sometimes are not so anonymous.

- Programmable
  - Tor has a Framework (**Stem** – Uses Control Port)

HOW DOES PYMULTITOR WORK?

- PyMultitor work with EventLoop (Gevent) and multiple Tor processing (Sub Processes).

- Each Tor process is responsible for the connection between a single IP address (Proxy) and the target. Furthermore, each Tor process has two addresses – an internet address (Socks 4a Proxy) and a management address.

- Each time the programs identifies that the IP is blocked, a new identity is requested from Tor meaning a new IP address is issued to this connection. The request that was blocked is re-sent and the testing process will continue.

FUTURE GOALS

- The main goal is to allow programmers to work with the PyMultitor framework with ease.
- Creating a Class that will manage an organized configuration, a Class that will manage performing actions and allow testing for known attacks like Brute-Force, Local File Inclusion (LFI), Cross Site Scripting (XSS), Fuzzing and more.
- Combining the Multi Processing ability with Gevent can significantly accelerate the work and allow using almost all the benefits of asynchronous programming.

Programming Concerns

SECTION

4.1

GLOBAL INTERPRETER LOCK (GIL)

What is the Global Interpreter Lock, or GIL?

A “mutex” that prevents multiple native threads from executing Python bytecodes at once.

This lock is necessary mainly because CPython's memory management is not thread-safe. (However, since GIL exists, other features have grown to depend on the guarantees that it enforces.)

GEVENT

gevent is a coroutine -based Python networking library that uses greenlet to provide a high-level synchronous API on top of the libev event loop.

Features include:

- Fast event loop based on libev (epoll on Linux, kqueue on FreeBSD).
- Lightweight execution units based on greenlet.
- API that re-uses concepts from the Python standard library (for example there are gevent.event.Events and gevent.queue.Queues).

STEM - NOT MY BUGS ☹

https://trac.torproject.org/projects/tor/ticket/10072

Error Message In Windows:

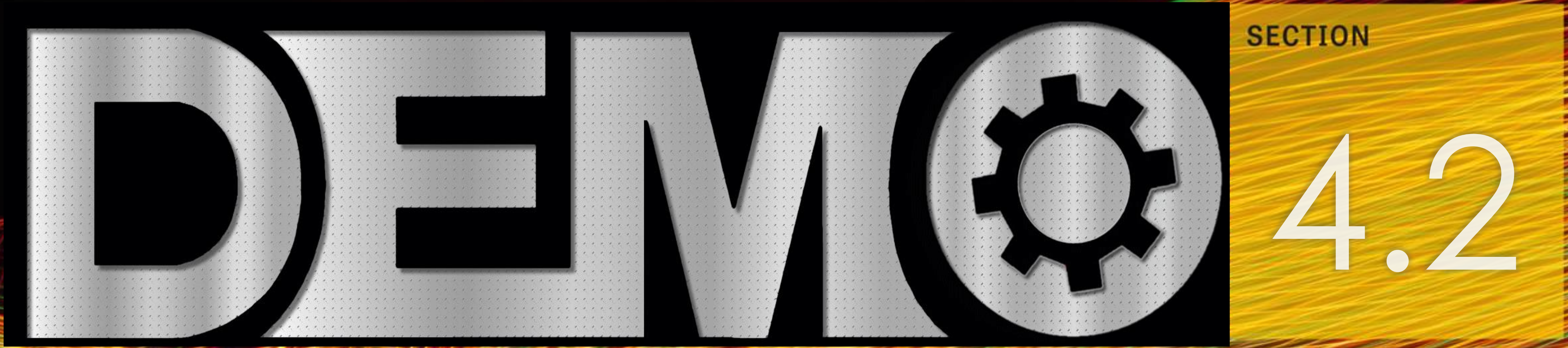
The Message => ImportError: No module named pwd

On Function => launch_tor_with_config

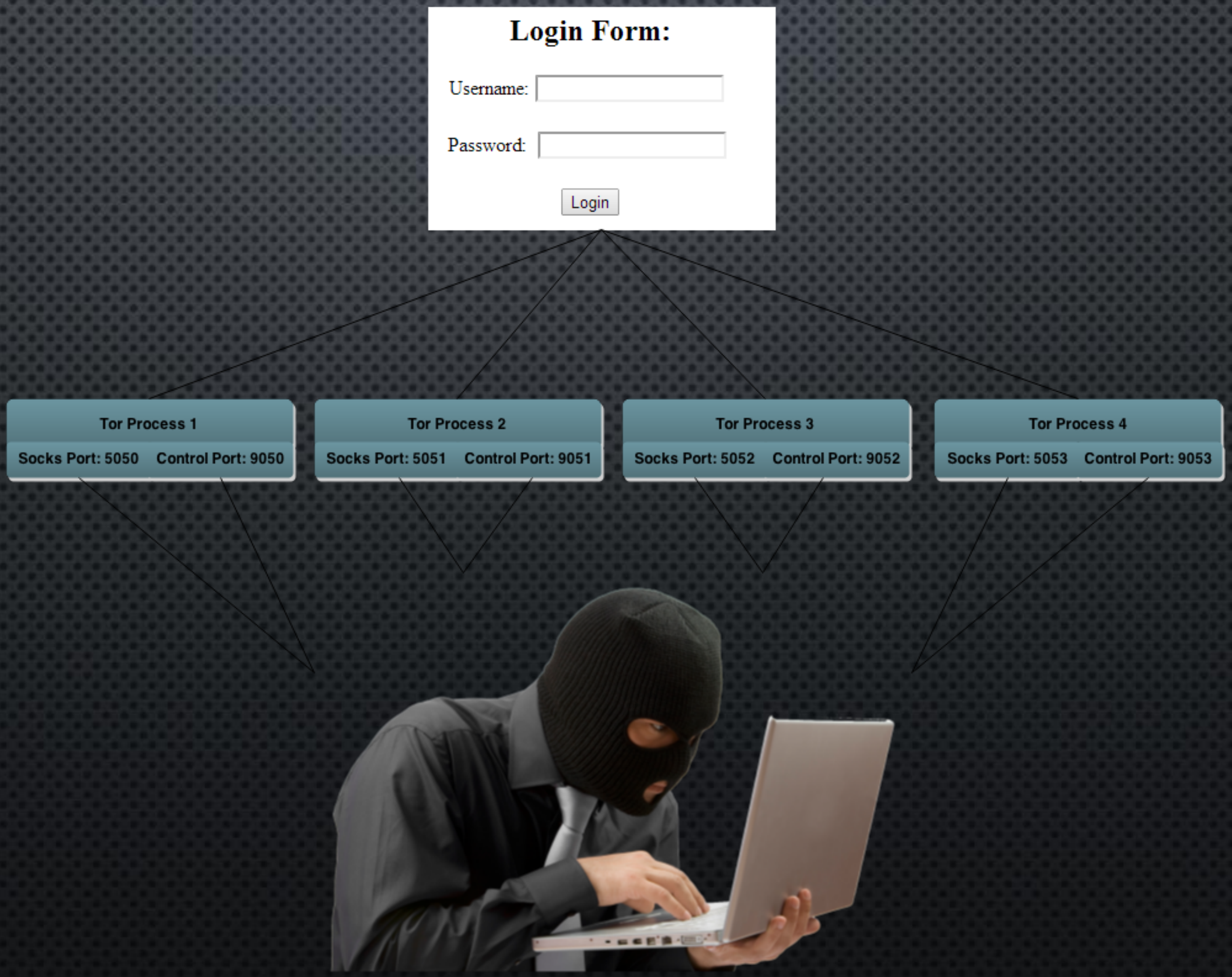
The Reason => Theres import of pwd lib on stem.util.system, pwd lib is not exist on windows.

Solution => if statement on the import / Try Except.

BRUTEFORCE DEMO



PYMULTITOR – IT'S DEMO TIME



Login Form:

Username:

Password:

Login

Tor Process 1

Socks Port: 5050 Control Port: 9050

Tor Process 2

Socks Port: 5051 Control Port: 9051

Tor Process 3

Socks Port: 5052 Control Port: 9052

Tor Process 4

Socks Port: 5053 Control Port: 9053

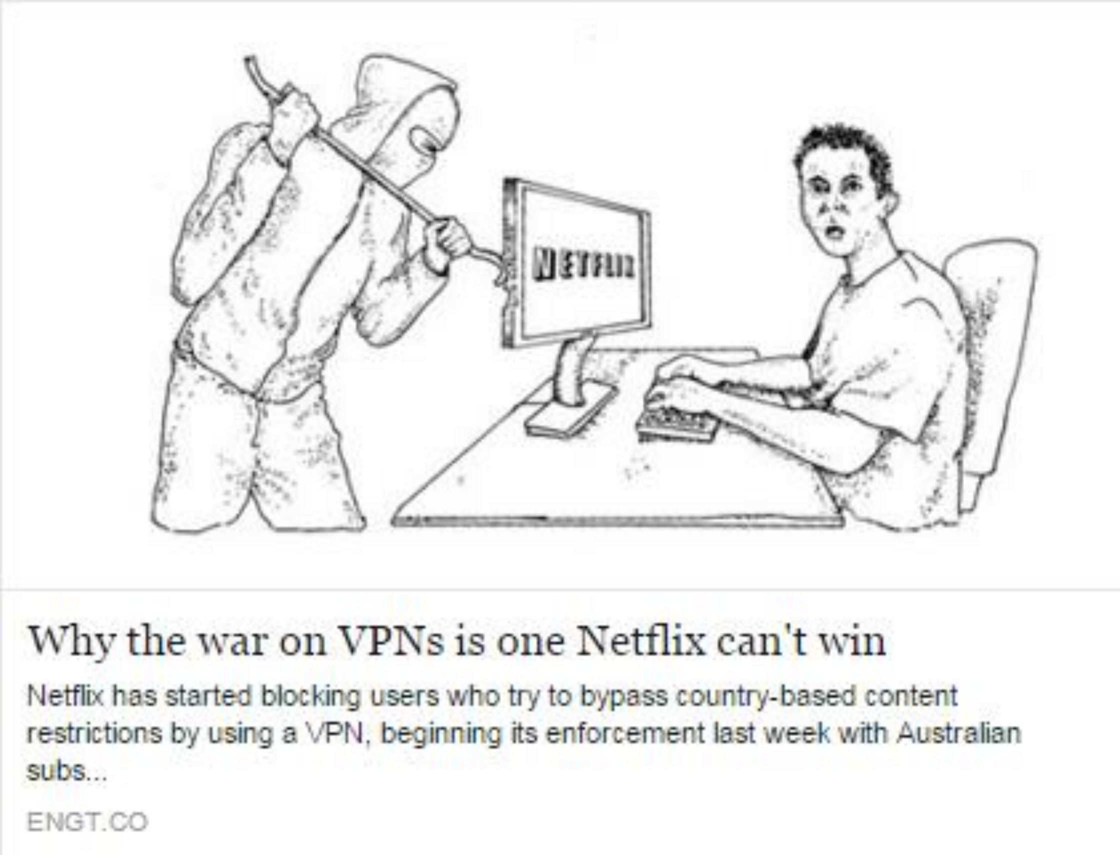
Can We Prevent It?

Does it refer only to tor?

SECTION

5

WE WILL SEE HOW IT GOES FOR NETFLIX…



Why the war on VPNs is one Netflix can't win

Netflix has started blocking users who try to bypass country-based content restrictions by using a VPN, beginning its enforcement last week with Australian subs...

ENGT.CO

DEFEND
THE NEW PERIMETER

Solutions for an application world.

devcentral.f5.com

T.Zait@f5.com