

## Leveraging Docker-based containers to teach cyber security

### Introduction

Teaching cyber security concepts in an effective way has always been a challenging task. Practically demonstrating the security concepts, threats and attacks in action is an attractive approach. In this work, we use Docker-based containers to demonstrate and teach various security threats using hands on approach.



### The Challenge

A need for practical approach to teach cyber security

- Must allow the user to visualize concepts.
- Must enable the user to 'learn by doing'.
- Easily configurable and accessible

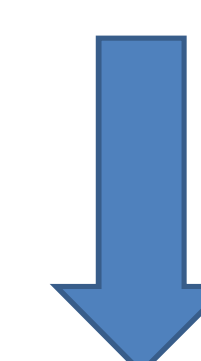
Cloud based

- Using elastic and scalable cloud resources
  - Support large number of users if required
- Operating System and Internet Browser Independent.



### Our Approach

- Dockerize different security related tools and concepts
- Use a cloud-based platform to allow user access to different dockerized security tools
- Allow the users to experience the security threats and problems themselves.



### Current Status

- 9 different scenarios available (more scenarios to be added).

<b>ArpSpoof</b> A demonstration of ARP table poisoning <a href="#">Learn more...</a>	<b>SSLStrip</b> A demonstration of HTTPS stripping attack <a href="#">Learn more...</a>	<b>HSTS</b> A demonstration of a web security policy <a href="#">Learn more...</a>	<b>HeartBleed Exploit</b> A demonstration of a recently patched OpenSSL vulnerability <a href="#">Learn more...</a>
<b>T-DNS: DNS over TCP and TLS</b> A demonstration of improved security for DNS queries <a href="#">Learn more...</a>	<b>LongTail SSH Honeypot</b> A demonstration of brute force attack logging <a href="#">Learn more...</a>	<b>Ofuzz Fuzzing framework</b> A demonstration of a flexible fuzzing platform <a href="#">Learn more...</a>	<b>SQL Injection</b> A demonstration of a code injection attack <a href="#">Learn More...</a>
<b>Padding Oracle Attack</b> Write and test code that conducts a Padding Oracle attack <a href="#">Learn More...</a>			

- Accessed by users from 4 different continents



### Comparative Analysis

- Our Docker-based Approach
- User-machine based



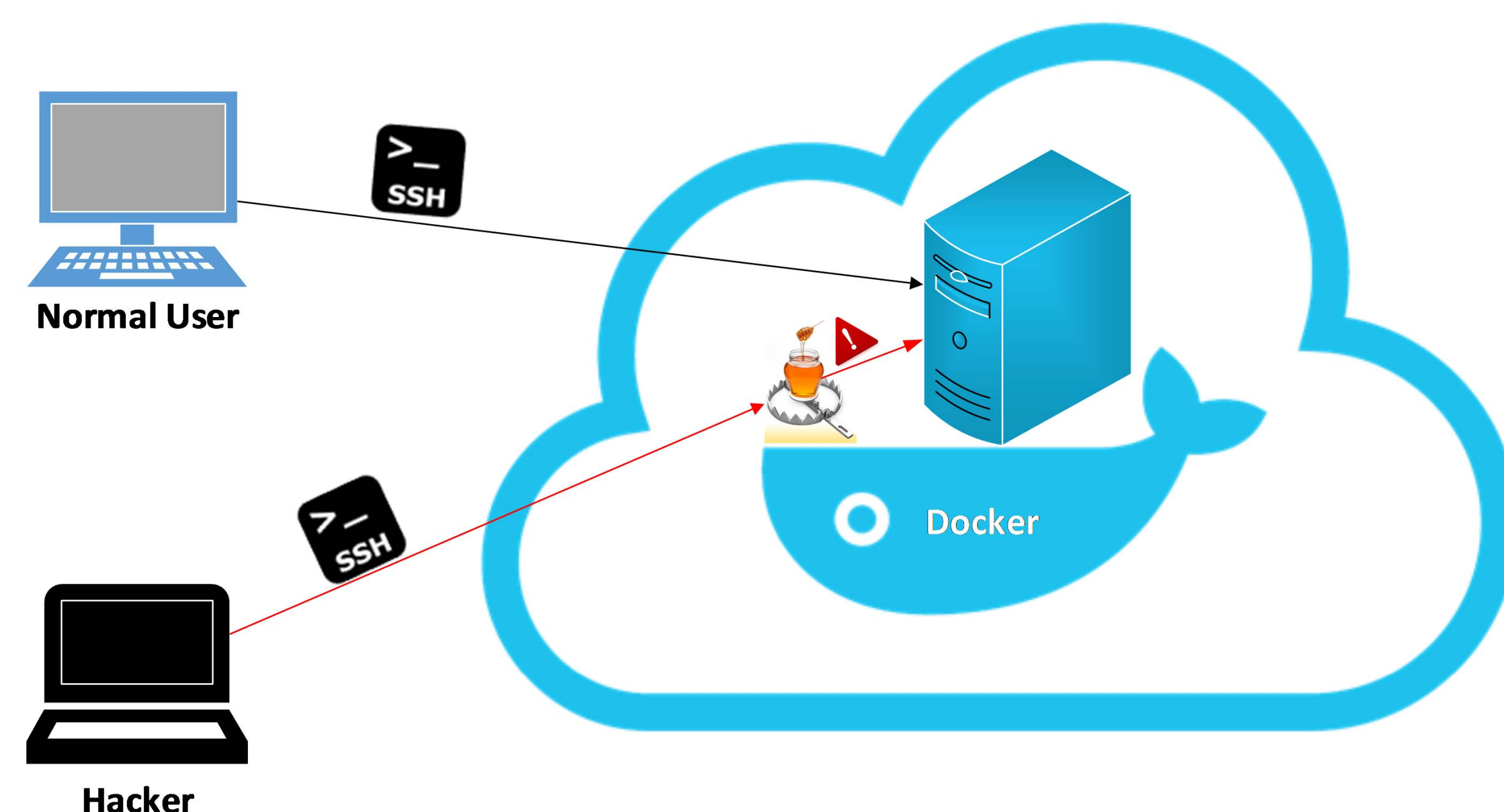
- Access our website through internet and use the tools.  
- User doesn't worry about security, and resources.



- Download and install the tools  
- Risk your computer's security  
- Allocate resources so high processing power required  
- Eliminate the risk once done.



### SSH Honeypot Example



The project is funded by IEEE Cyber Security Initiative and available at <http://try.cybersecurity.ieee.org/>