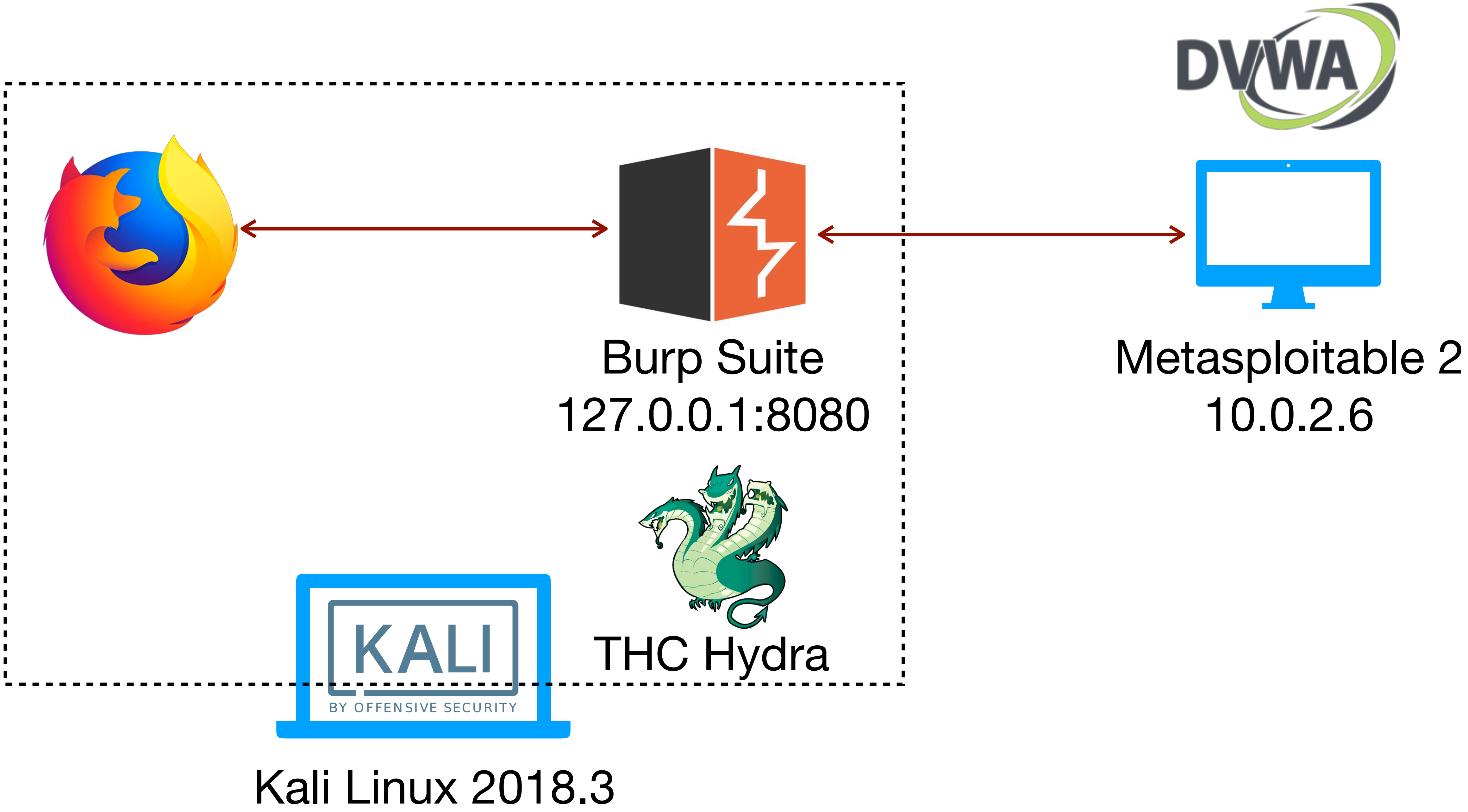
Attacking Web-based Applications

WIC3004 Computer Penetration

Faculty of Computer Science and Information Technology
Semester 1, 2018/2019

UNIVERSITI
MALAYA

The Setup



Burp Suite
127.0.0.1:8080

Metasploitable 2
10.0.2.6

THC Hydra

Kali Linux 2018.3

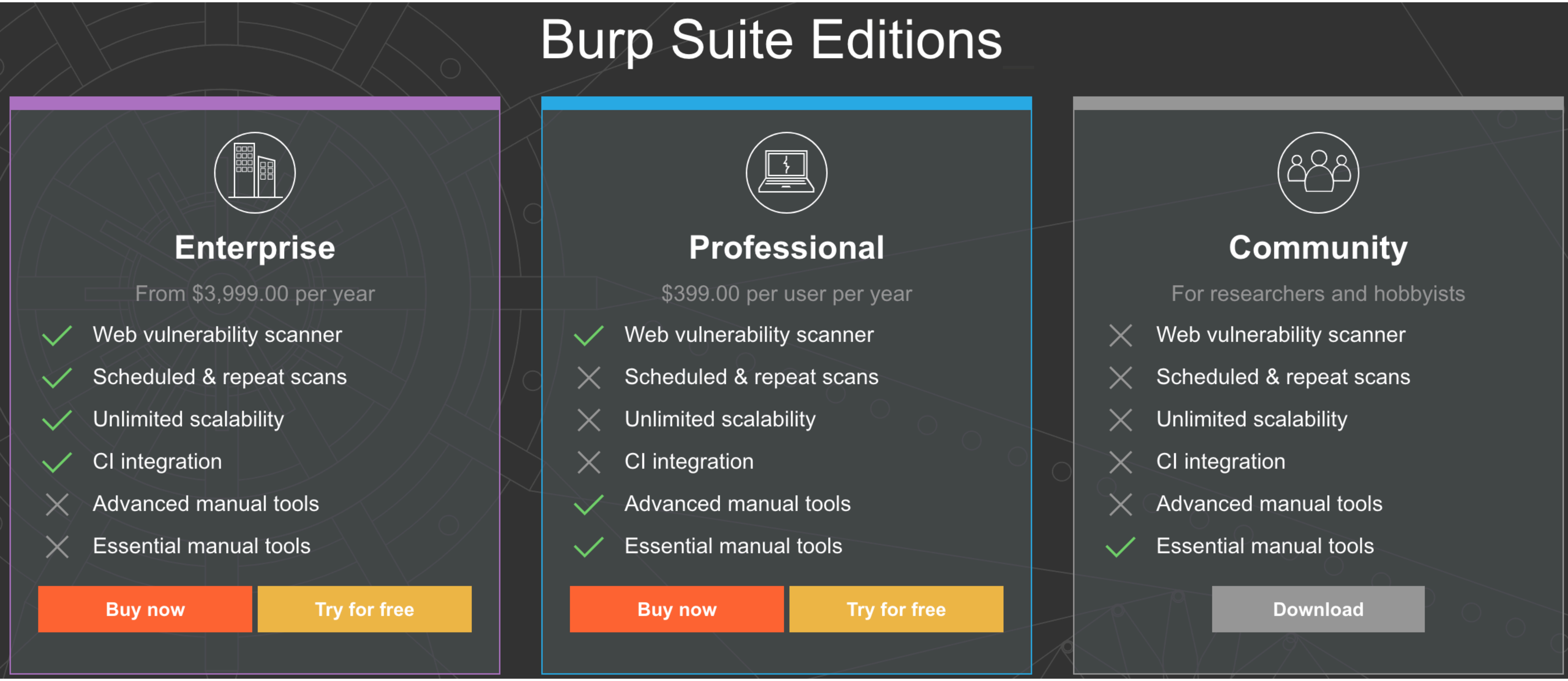
Note that the IP address of your Metasploitable machine may differ

Burp Suite

- Burp Suite is a tool for testing Web application security
- Burp Suite Community Edition is bundled with Kali Linux 2018.3
- Enterprise and Professional Editions require license
- In our Lab exercise, Burp Suite will act as a proxy between Firefox and the DVWA

https://portswigger.net/burp

Burp Suite



Burp Suite Editions

	Enterprise	Professional	Community
	From $3,999.00 per year	$399.00 per user per year	For researchers and hobbyists
Web vulnerability scanner	✓	✓	✗
Scheduled & repeat scans	✓	✗	✗
Unlimited scalability	✓	✗	✗
CI integration	✓	✗	✗
Advanced manual tools	✗	✓	✗
Essential manual tools	✗	✓	✓

Information as at 10 December 2018, https://portswigger.net/burp

Damn Vulnerable Web Application (DVWA)

- Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable
- Main goals:
  - to be an aid for security professionals to test their skills and tools in a legal environment,
  - help web developers better understand the processes of securing web applications,
  - and aid teachers/students to teach/learn web application security in a class room environment

Description obtained from http://www.dvwa.co.uk/

Damn Vulnerable Web Application (DVWA)

- Default username: admin
- Default password: password
- DVWA is already bundled with Metasploitable 2

Description obtained from http://www.dvwa.co.uk/

THC Hydra

- THC Hydra is a tool to guess/crack valid username/password pairs
- In our Lab exercise, Hydra will be used to crack the password of a specific user
- Hydra requires
    - HTTP method (e.g. POST, GET)
    - address of login page
    - failed login message

https://github.com/vanhauser-thc/thc-hydra