KF5002 Web Programming
Suggestions for tutorial work

The Royal Academy of Engineering funded a Visiting Professorship in Practical Cybersecurity Insights at Northumbria University, 2019–2022. These slides are a slightly modified version of those delivered, intended to be available after the project has ended

Web `https://green-pike.co.uk/nvp`
Email p.brooke@northumbria.ac.uk (until it stops working. . .)
phil@green-pike.co.uk

These are “extension” suggestions. You should make sure you’ve completed work from your tutors first

The links are to external sites that appear helpful: they may change over time!

Software requirements

Some suggestions require additional software. Admin *a.k.a.* root *a.k.a.* superuser rights are particularly helpful!

Virtual machines

are a good way to explore computer science and security concepts

Windows VirtualBox is free and easy to use

Linux VirtualBox is also available for Linux, although some recent distributions may be problematic.
Virt-manager is a good alternative

Caution

Do not scan or tamper with systems that you don't control. . .

. . . unless you have permission from the system owner

1. Injection attacks

Three external resources:

1. `https://www.guru99.com/learn-sql-injection-with-practical-example.html`
2. `http://www.unixwiz.net/techtips/sql-injection.html`
3. `https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OTG-INPVAL-005)`

Practical suggestion

1. Set up a simple database with two tables
2. Set up a web form that should update the first table
3. Experiment with inputs that affect the second table

([Jul 2020] See the PHP resources near the source of these slides!)

2. Password crackers

First, don't use MD5 — it's too weak — we're using it here because of that weakness

Practical suggestion

This requires a typical Linux installation, *e.g.*, Kali, Debian, Ubuntu

1. Create a password file: some passwords should be very short (length 6) and some a little more
2. Use John the Ripper (Debian package "john") and/or hashcat
3. Hash them using md5sum
4. Try to crack them

(Examples on next slide)

2. Password crackers (cont'd)

(The commands below should be entered on a single line)

Create 10 passwords, length 6, hashed with MD5

```
for n in $(pwgen 6 10); do echo -n "$n" | md5sum
  | cut -f1 -d' ' ; done
```

Try to crack them:

```
hashcat --force -1 '?l?u?d'
  --increment --increment-min 6 --increment-max 6
  -m 0 -a 3 theHashFile '?1?1?1?1?1?1?1'
```

3. Password salting

An example salted MD5 hashed password:

`7dd0bea27cbbdf47c60c62accec81247:Aimeyu8O`

- In that line, `:` separates the hash from the salt
- The salt is `Aimeyu8O`

Repeat the previous exercise, but use salted passwords

```
for n in $(pwgen 6 10); do
  s=$(pwgen 8 1);
  echo -n "$n$s" | md5sum | cut -f1 -d" "
  | tr -d '\n'; echo ":$s";done
```

You'll need to change `-m 0` to `-m 10` for salted MD5

4. Port security

1. Identifying ports
   The "official" allocation of Internet ports is controlled by IANA
   See `https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml`
2. See if you can locate these common TCP ports: 443, 25, 143, 587. What are they used for?
3. Note: just because someone *says* you should a particular port number doesn't mean you have to... it's common to put SSH servers on complete different ports

4. Port security (cont'd)

nmap is an excellent tool for network recon and for checking particular hosts. Example:

```
phil@host:~$ nmap -sT  [snip]
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-08 16:17 GMT
Nmap scan report for [snip] ([snip])
Host is up (0.026s latency).
Other addresses for [snip] (not scanned): [snip]
rDNS record for [snip]: [snip]
Not shown: 993 filtered ports
PORT    STATE  SERVICE
25/tcp  open   smtp
53/tcp  closed domain
80/tcp  open   http
88/tcp  closed kerberos-sec
143/tcp open   imap
443/tcp open   https
587/tcp open   submission

Nmap done: 1 IP address (1 host up) scanned in 4.75 seconds

phil@host:~$ sudo nmap -sU  [snip]
[repeated output snipped]
Not shown: 998 open|filtered ports
PORT   STATE    SERVICE
53/udp filtered domain
88/udp closed   kerberos-sec

Nmap done: 1 IP address (1 host up) scanned in 25.11 seconds
```

4. Port security (cont'd)

Exercise

Work out the meaning of each result from nmap (on the previous slide)!

5. OpenVAS

OpenVAS is a free fork of Nessus

This is a *large* tool that is primarily of interest to security specialists. Setting up takes a while (usually longer than a tutorial!)

See `http://www.openvas.org/`

The end

Web	`https://green-pike.co.uk/nvp`
Email	p.brooke@northumbria.ac.uk (until it stops working. . .)
	phil@green-pike.co.uk

Phil Brooke
A *Royal Academy of Engineering Visiting Professor* in Practical Cybersecurity Insights
Northumbria University