

CMSC389R

Penetration Testing II



COMPUTER SCIENCE
UNIVERSITY OF MARYLAND



miscellanea on assignments

- Questions about a grade/regrade request? Talk to us after class.
- For programming: **Always** submit your code! We need to see *how* you're getting your answers.
- For answers: **Always** give us your reasoning! Use bullet points if it helps.

recap

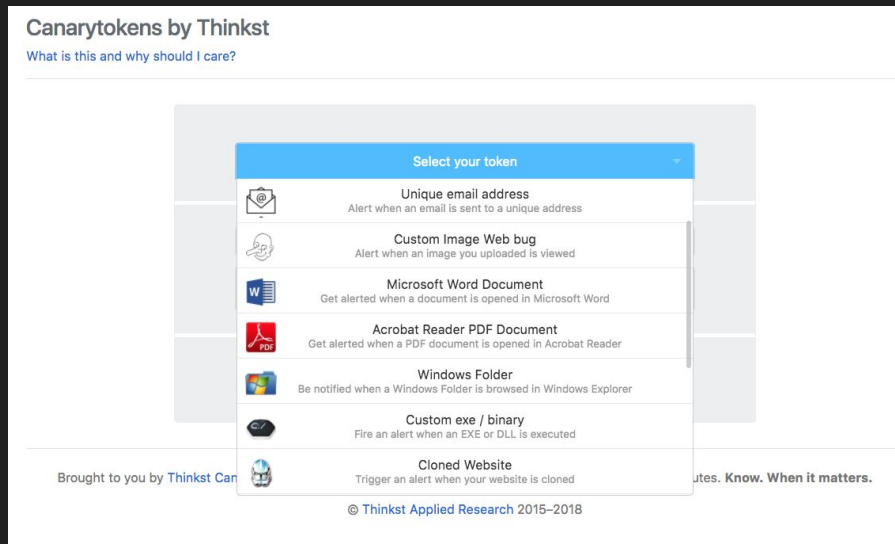
HW 3

HW 2 regrade requests (deadline is Wednesday
11:59 PM)

Questions?

Demo: Canarytokens

- Canarytokens: used to detect an intrusion or to discover IP address information and User Agent info
 - <https://canarytokens.org>



Demo: URITeller

- URITeller: similar to Canarytokens, used to detect IP address and User Agent info
 - <https://uriteller.io>

URI:teller



Monitoring visits to URL

https://uriteller.io/zQ6rZCBVql1-_kzuK7GovQ [copy](#)

This is your **trap URL**. Copy-paste it to your favorite messaging app, URL shortener or social network site. This **monitor page** shows who visits the trap.

Visits

live updates on

Time	IP	ASN	User Agent
2018-02-21 01:11:43 a few seconds ago	 24.104. [REDACTED]	7922 COMCAST-7922 - Comcast Cable Communications, LLC	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_1) AppleWebKit/601.2.4 (KHTML, like Gecko) Version/9.0.1 Safari/601.2.4 facebookexternalhit/1.1 FacebookTwitterbot/1.0
2018-02-21 01:10:25 2 minutes ago	 107.20.5.123	14618 AMAZON-AES - Amazon.com, Inc.	bitlybot/3.0 (+http://bit.ly/)

URL auto-preview
iOS iMessage

Bit.ly URL
shortening service

metasploit

- Powerful pentesting tool developed by [rapid7](#)
 - Ships with Kali
 - Written in Ruby
 - Expandable (add new modules)
- Command line interface
 - Tab-autocomplete
 - Ctrl-r reverse history search/Ctrl-l clear/etc...
 - Execute shell commands on host OS

metasploit

- Typically enables a listening service on attackers machine as a command and control (C2)
- Comes with:
 - Auxiliary (ie. scanning) tools
 - Exploit code
 - Post-exploit process
- We will only be touching the surface
 - [Learn more](#)
 - See chapter 8 Gray Hat Hacking

msfconsole

- Let's start metasploit
- In Kali, open the terminal and type:

```
$ msfconsole
```


msfconsole

Lists exploits:

```
$ show exploits
```

Lists payloads (what to do after exploit):

```
$ show payloads
```

msfconsole

Searching for exploits:

```
$ search flash
```

```
$ search heartbleed
```

Using an exploit:

```
$ use auxiliary/scanner/ssl/openssl_heartbleed
```

msfconsole

List configurable options for exploit:

```
$ show options
```

Set remote host IP address:

```
$ set RHOSTS <ip address here>
```

Enable verbose output:

```
$ set VERBOSE true
```

msfconsole

Exploit!

```
$ exploit
```

**HW 4*

Demo: metasploit

- If you want to try this yourself, download the [metasploitable2](#) vulnerable VM

Demo: armitage

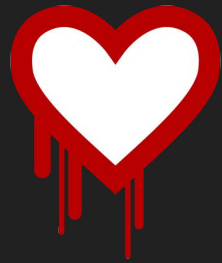
- Graphical front-end for metasploit
- Easy, one-click hacking
- www.fastandeasyhacking.com

what is metasploit actually doing?

- Provides an interface for exploits that take advantage of certain software vulnerabilities such as:
 - Overflows (ie. Buffer/Integer/Heap/etc)
 - Injection (ie. Command/etc)
 - Backdoors
 - Weak configuration
 - ...

Example: Heartbleed (CVE-2014-0160)

- Buffer over-read vulnerability in OpenSSL (crypto lib)
 - “allows **anyone** on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software”
 - OpenSSL 1.0.1 through 1.0.1f (inclusive)
- More info: <http://heartbleed.com>



how?

```
/* Read type and payload  
length first */
```

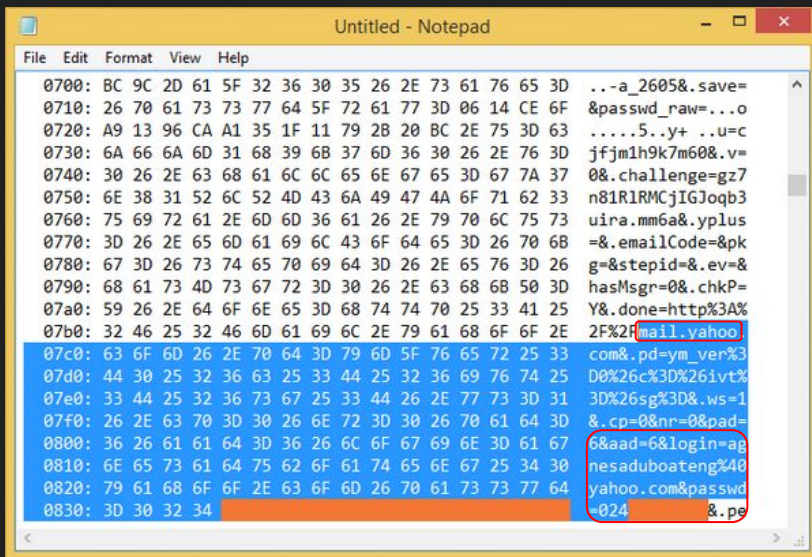
```
hbtype = *p++;  
n2s(p, payload);  
p1 = p;
```

```
/* Enter response type, length  
and copy payload */
```

```
*bp++ = TLS1_HB_RESPONSE;  
s2n(payload, bp);  
memcpy(bp, p1, payload);
```



how?



```
0700: BC 9C 2D 61 5F 32 36 30 35 26 2E 73 61 76 65 3D ..-a_2605&.save=
0710: 26 70 61 73 73 77 64 5F 72 61 77 3D 06 14 CE 6F &passwd_raw=...o
0720: A9 13 96 CA A1 35 1F 11 79 28 20 BC 2E 75 3D 63 .....5..y+ ..u=c
0730: 6A 66 6A 6D 31 68 39 68 37 6D 36 30 26 2E 76 3D jfjm1h9k7m60&.v=
0740: 30 26 2E 63 68 61 6C 6C 65 6E 67 65 3D 67 7A 37 0&.challenge=gz7
0750: 6E 38 31 52 6C 52 4D 43 6A 49 47 4A 6F 71 62 33 n81R1RMCjIGJoqb3
0760: 75 69 72 61 2E 6D 6D 36 61 26 2E 79 70 6C 75 73 uira.mm6a&.yplus
0770: 3D 26 2E 65 6D 61 69 6C 43 6F 64 65 3D 26 70 68 =&.emailCode=&pk
0780: 67 3D 26 73 74 65 70 69 64 3D 26 2E 65 76 3D 26 g=&stepid=&.ev=&
0790: 68 61 73 4D 73 67 72 3D 30 26 2E 63 68 68 50 3D hasMsgnr=0&.chkP=
07a0: 59 26 2E 64 6F 6E 65 3D 68 74 74 70 25 33 41 25 Y&.done=http%3A%
07b0: 32 46 25 32 46 6D 61 69 6C 2E 79 61 68 6F 6F 2E 2F%2Fmail.yahoo
07c0: 63 6F 6D 26 2E 70 64 3D 79 6D 5F 76 65 72 25 33 com&.pd=ym_ver%3
07d0: 44 30 25 32 36 63 25 33 44 25 32 36 69 76 74 25 D0%26c%3D%26ivt%
07e0: 33 44 25 32 36 73 67 25 33 44 26 2E 77 73 3D 31 3D%26sg%3D&.ws=1
07f0: 26 2E 63 70 3D 30 26 6E 72 3D 30 26 70 61 64 3D &.cp=0&nr=0&pad=
0800: 36 26 61 61 64 3D 36 26 6C 6F 67 69 6E 3D 61 67 6&aad=6&login=ag
0810: 6E 65 73 61 64 75 62 6F 61 74 65 6E 67 25 34 30 nesaduboaeng%40
0820: 79 61 68 6F 6F 2E 63 6F 6D 26 70 61 73 73 77 64 yahoo.com&passwd
0830: 3D 30 32 34 024 &.pe
```

/* Enter response type, length
and copy payload */

```
*bp++ = TLS1_HB_RESPONSE;  
s2n(payload, bp);  
memcpy(bp, pl, payload);
```

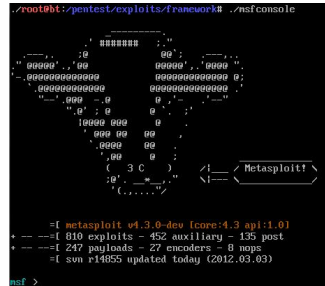


is metasploit necessary?

- No, not really
- Many PoCs available online that don't require metasploit

WHO WOULD WIN?

Large pentesting tool



One nifty python script



your turn

- Exploit CVE-2017-5638 to gain access to Mark's server at:

<http://briong.com:8080>

In this exercise, you will be practicing:

1. Finding exploit scripts online (ie. exploit-db)
2. Running the scripts against our live target
3. Maybe find a flag?

homework #4

has been posted.

Let us know if you have any questions!

This assignment has two parts.

It is due by 3/1 at 11:59 PM.