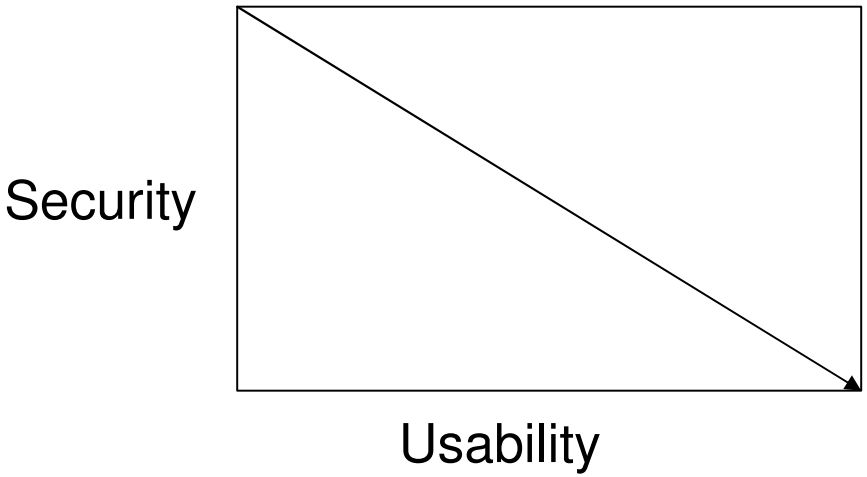
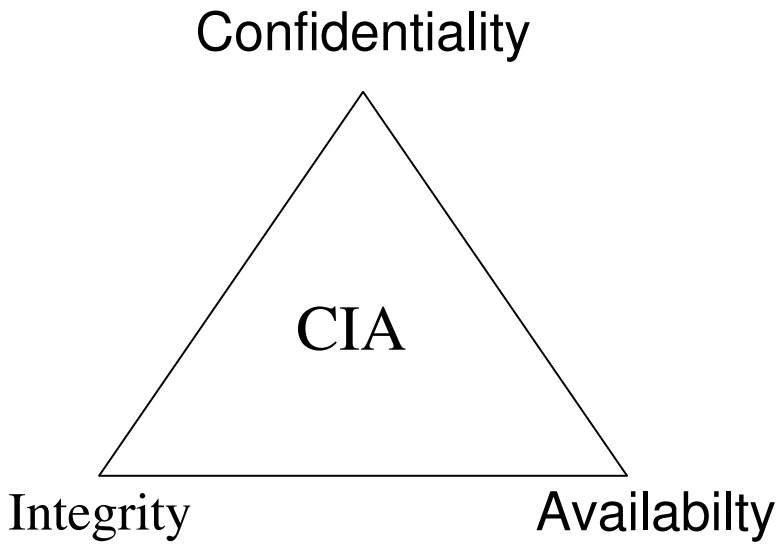
Ethical Hacking - Reconnaisance

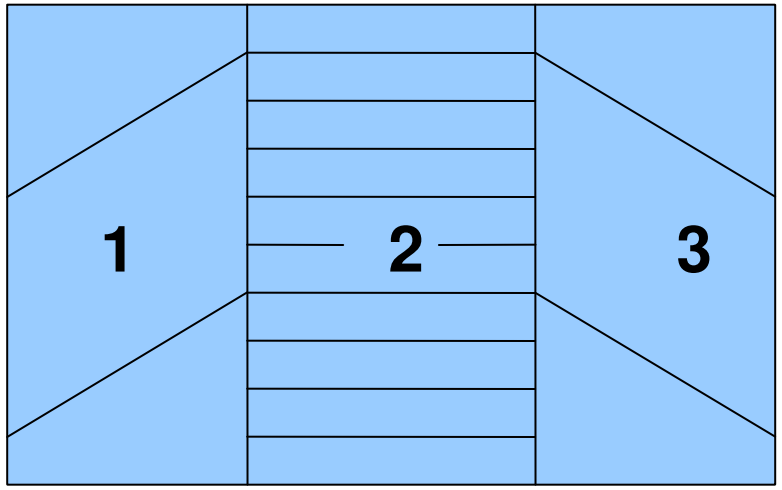
By Nic Maurel

- What is Ethical Hacking?
- Why Ethical Hacking?
- What do companies aim to protect?





- What kind of tests do we do on the “Target of Evaluation”?
  - Black Box Test
  - White Box Test
  - Grey Box Test
- Types of Ethical Hackers
  - Whitehat Hackers
  - Blackhat Hackers
  - Greyhat Hackers



1 – Pre-Assessement

2 – Assessment Phase

3 – Post Assessment

- Who are we up against?
  - Phreakers
  - Script kiddies
  - Disgruntled Employees
  - Cyber Terrorists Hacktivists
  - Software Crackers/Hackers
  - System Crackers/Hackers
  - Whackers

- Historical Hackers
- John Draper -AKA “Captain Crunch”
- Kevin Mitnick – first hacker to hit the FBI wanted list
- Vladimir Levin – siphoned off large amounts of money from citibank
- Jonathan James – first juvenile hacker to be arrested at age 16
- Adrian Lamo – Broke into the New York Times and Microsoft

- Scope of Attack for TOE
  - Insider Attack
  - Outside Attack
  - Stolen Equipment Attack
  - Physical Entry
  - Bypass authenication
  - Social Engineering

- Hacker Methodology
- Reconnaisance
- Scanning and Enumeration
  - Active scanning
  - Passive scanning
- Gaining Access
- Priveledge Escalation
- Maintaining Access
- Covering Tracks placing backdoors

- # Reconnaissance – Casing the Joint
- Search the fine web (STFW) :
- Google – the hackers big gun

  Google Cached Copies

  site:www.test.co.za

  insite:www.test.co.za "this report was generated by nessus"

  filetype:xls

  Inurl:search-text

  Link:www.test.co.za

  Intitle:Welcome to IIS4.0
- Search Company website – View source code
- Job boards and user groups and forums
- EDGAR Database - www.sec.gov
- www.archive.org

- # Whois – Registrar information

- ARIN – www.arin.net - North South America and Subsaharan Africa
- APNIC – www.apnic.net - Asia Pacific
- RIPE – www.ripe.net - Europe Middle East
- LACNIC - www.lacnic.net – Latin America and Carribean
- AfriNIC – Planned to supoort Africa

- # Tools

  www.samspade.org

  Whois client – linux

  www.dnsstuff.com

  www.allwhois.com

  www.ipaddresslocation.org

- # DNS Interrogation
- Search for SOA, A, MX, SRV, CNAME and PTR records.
- Nslookup www.test.co.za
- Nslookup 192.168.0.3
- Use address to find Network ranges with whois
- Lookup addresses below and above eg. 192.168.0.2 and 192.168.0.4
- Dig -t ANY test.co.za
- Try zone transfers
- Look for common names eg. Smtp, pop, pop3, imap, proxy, server, mail, dbn, durban.

- Host Detection
- Port Detection
- Service Detection
- Check for Vulnerabilites in services or OS

PASSIVE OS DETECTION

- The way that an OS has been implemented in the network protocol stack can be differentiated

```
IP  IP  DF  IP  TCP  TCP
len     id   set TTL seq win Operating System
===     ==   === === === === ====================
40B     >0   yes 64  0   0   Solaris8
40B     >0   no  128 0   0   WinME, Win2K Server
40B     =0   yes 255 0   0   RedHat Linux 2.4.2
40B     >0   no  255 0   0   RedHat Linux 2.0.30
40B     >0   no  60  0   0   AIX Version 4
```

- POF is a passive OS detection tool which can automate the process

Banner Grabbing

- Telnet
- Netcat
- Stunnel
- Amap

Examples of Banner Grabbing

```
telnet 19x.xxx.xxx.xxx 80
Trying 19x.xxx.xxx.xx...
Connected to 19x.xxx.xxx.xxx (19x.xxx.xxx.xxx).
Escape character is '^]'.
GET / HTTP/1.0


HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Thu, 14 Jun 2007 06:53:22 GMT
X-Powered-By: ASP.NET
Connection: Keep-Alive
Content-Length: 1270
Content-Type: text/html
Cache-control: private
```

```
[watts@myhost ~watts]$ telnet
some.mail.server.out.there 25

Trying 10.10.10.10...

Connected to some.where.out.there
(10.10.10.10).

Escape character is '^]'.

220 some.where.out.there ESMTP Exim 1.73
#1 Sat, 12 Jan 2002
 20:46:22 -0800
```

Network Mapping

- Traceroute/tracert
- ping
- Tcptraceroute
- Paratrace

Thank you for Listening

- Paratrace - http://www.doxpara.com/code/paketto-1.10.tar.gz
- Tcp traceroute - http://michael.toren.net/code/tcptraceroute/tcptraceroute-1.4.tar.gz
- Net cat for windows - http://www.vulnwatch.org/netcat/nc111nt.zip
- P0f v2 - http://lcamtuf.coredump.cx/p0f.tgz
- johhny.ihackstuff.com