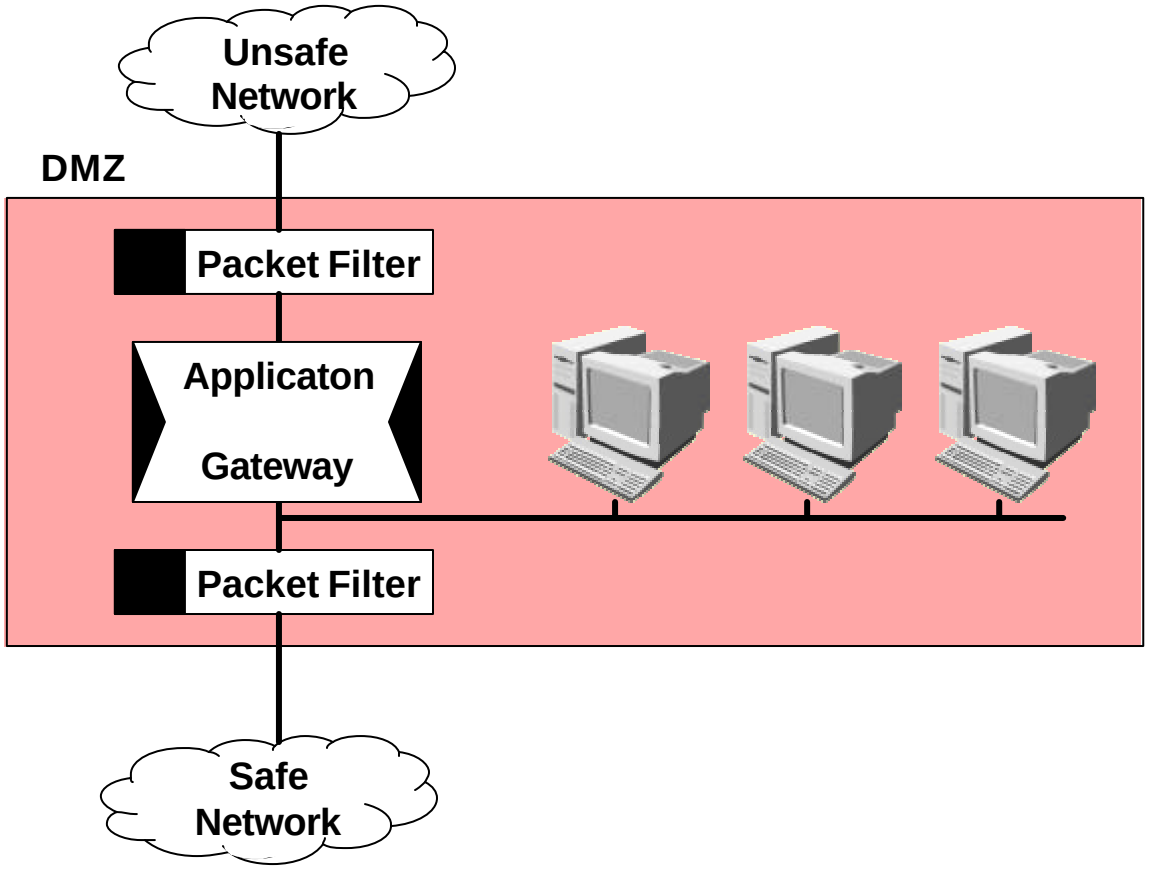
hack the net

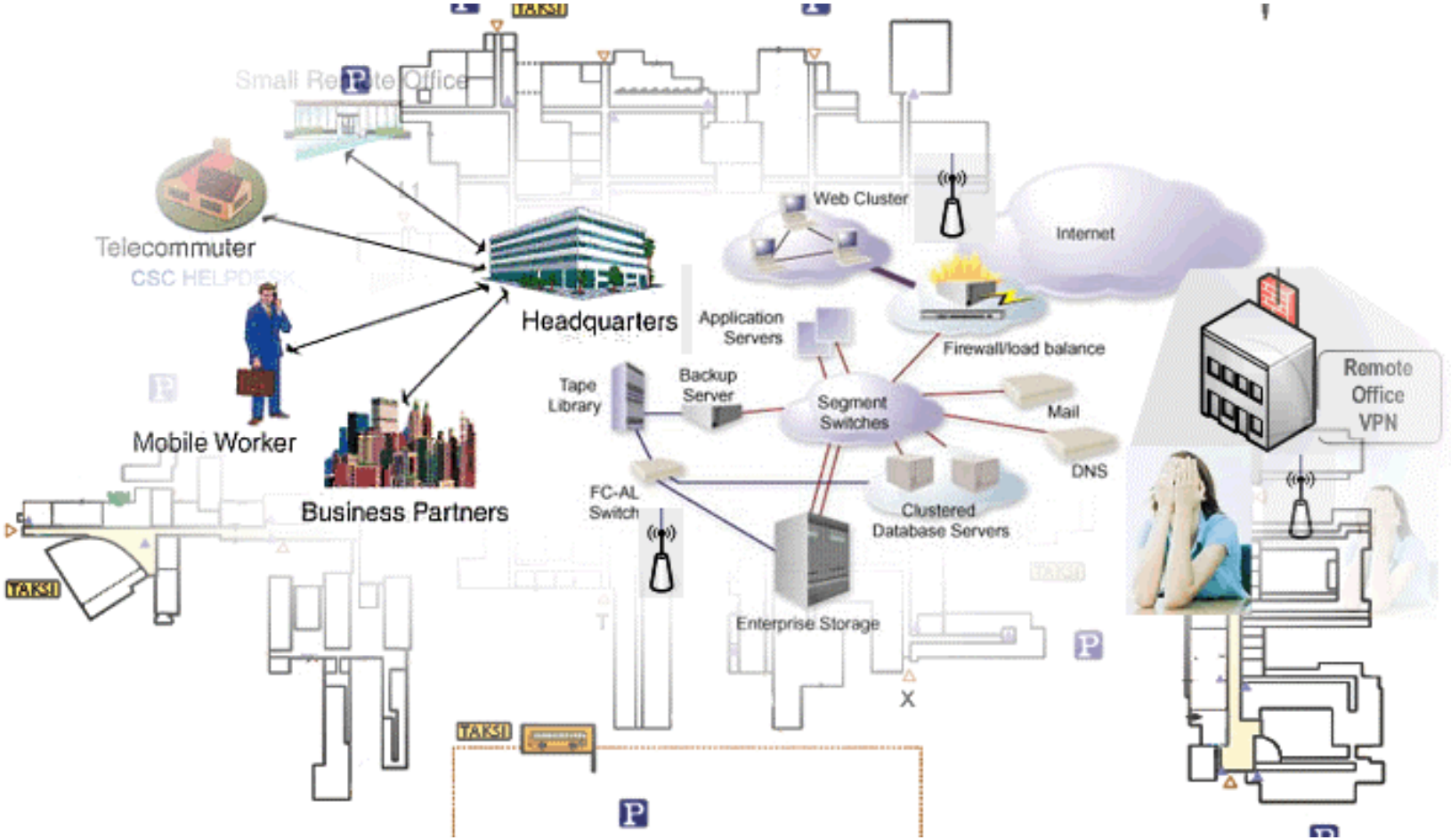

ID#: 31337
Name: Scriptkiddie
Federal Bureau of Investigation
(c) by Krycek


BlackHat
black as u can be

Hack the Net


Unsafe
Network
DMZ
Packet Filter
Applicaton
Gateway
Packet Filter
Safe
Network

Hack the Net


Small Remote Office
Telecommuter
CSC HELPDESK
Mobile Worker
Business Partners
Headquarters
Web Cluster
Internet
Application Servers
Firewall/load balance
Tape Library
Backup Server
Segment Switches
Mail
DNS
FC-AL Switch
Clustered Database Servers
Enterprise Storage
Remote Office VPN

goals and motivations
-- be sure to know what you want --

- know about your motivations
- - hack for money
- - hack for political motivations
- - hack for fame and honor
- - hack for technical survey

- define your goals
- - deface a website
- - bring down a service, host or network (Denial of Service)
- - own the box - to prepare an advanced attack
- - steal information's / documents
- - modify information's for your advantage

information gathering
-- know your enemy like yourself --

- visit targets websites
- review HTML Code, JavaScript and Comments & robots.txt
- search for passwords, hidden directories, contact names

- whois request at the Network Information Centre
- receive information about IP address ranges
- Names and EMail addresses of responsibles

- DNS Lookup
- use nslookup tools to receive informations about DNS- & EMAIL Server, looking for names like oracle, TestLinux, ...
- try a zone transfer

information gathering
-- know your enemy like yourself --

www.dns.lu

Domain name: hack.lu
Domain name holder:
CSRRT-LU ASBL,
2 rue de la Paix
L - 3541 Dudelange
Administrative Contact:
Arbogast Fred
CSRRT-LU ASBL,
2 rue de la Paix
L - 3541 Dudelange
fred@csrrt.org.lu
Technical Contact:
Dulaunoy Alexandre
10 rue du Faubourg
B - 6811 Les Bulles- Chiny
adulau@foo.be
Name Servers:
ns0.freeblind.net
ns1.freeblind.net

Nslookup

```
> server ns0.freeblind.net
Default Server:  ns0.freeblind.net
Address:  158.64.24.250

> set type=ANY
> hack.lu
Server:  ns0.freeblind.net
Address:  158.64.24.250
hack.lu nameserver = ns0.freeblind.net
hack.lu nameserver = ns1.freeblind.net
hack.lu internet address = 213.169.96.28
hack.lu MX preference =
     10, mail exchanger = mail.hack.lu
hack.lu nameserver = ns0.freeblind.net
hack.lu nameserver = ns1.freeblind.net
ns0.freeblind.net
     internet address = 158.64.24.250
ns1.freeblind.net
     internet address = 158.64.24.251
mail.hack.lu
     internet address = 213.169.96.28
```

information gathering
-- know your enemy like yourself --

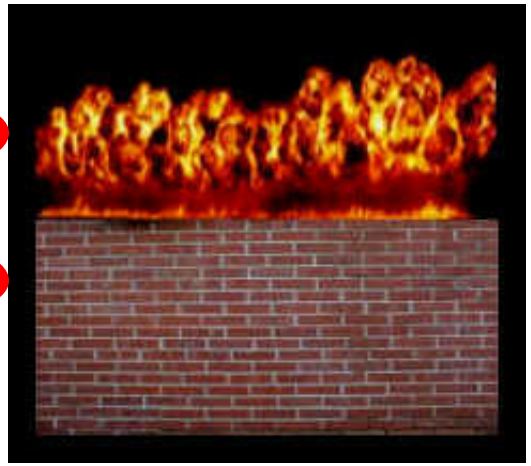
```
www.ripe.de
   inetnum:      213.169.96.0 -   213.169.127.255
   netname:      LU-ASTRANET-20021104
   descr:        SESM S.A. (Astra-Net)
   country:      LU
   address:      SESM S.A.
                 Chateau de Betzdorf,
                 L-6815 Betzdorf
                 G.-D. Luxembourg,
   phone:        +352 710 725 242
   phone:        +352 710 725 677
   fax-no:       +352 710 725 482
   e-mail:       thomas.graf@ses-astra.com
   e-mail:       francois.claire@ses-astra.com
```

information gathering
-- know your enemy like yourself --

- footprinting @ google
- news group articles of employees `author:<@targetdomain>`
- search business partners `link:<targetdomain>`
- `site:<targetdomain> intitle:index.of`
- `site:<targetdomain> error | warning`
- `site:<targetdomain> login | logon`
- `site:<targetdomain> username | userid`
- `site:<targetdomain> password`
- `site:<targetdomain> admin | administrator`
- `site:<targetdomain> inurl:backup | inurl:bak`
- `site:<targetdomain> intranet`

non - internet attacks
-- bypass the firewall --

hack the net



non - internet attacks
-- bypass the firewall --

- try to physically enter the target building
- attack the WLAN (Wireless LAN)
- War Dialling
- Social Engineering
- Dumpster Diving

  Quotation Bill Gates in: Susan Lammers; Programmers at Work Tempus Books; Reissue Edition, 1989

  „No, the best way to prepare is to write programs, and to study great programs that other people have written. In my case, I went to the garbage cans at the Computer Science Centre and I fished out listings of their operating system.“

internet based attacks
-- preperation --

- anonymity don’t exists
  - break systems in differrent countryies / time zones
  - install network multipurpose tools like netcat or backdoors
  - hop from host to host to get anonymity

- mapping of the target network
  - use system tools like traceroute & ping
  - identify network devices like firewalls & routers
  - identify servers; map network and subnet structure

- identify active services
  - portscan; nmap; Stealth-, ACK-, Null-, Xmas- Scan
  - identify operating system & services
  - identify application behind services & patch level

internet based attacks
-- be silent --

- prepare attack
  - research on internet for known security holes
  - default passwords; common miss configurations
  - setup a test environment to practice the attack
  - ideal: fire one single attack

- after a successful initial attack
  - hide the tracks from logfiles
  - expand local rights; find vulnerabilities in network
  - install rootkits, steal password database, start network sniffer
  - try same password on other systems
  - find problems in topology (expl. dual homed hosts)
  - try to attack the private network

primary target webserver
-- why they are so vulnerable --

- complex application
- multiple subsystems:
  application server, scripts, sql-server
- self made applications:
  programmer don’ t know how to write secure code
- Shell-Command-Injection:
  bypass commands trough the shell
  Input: "Alice; rm - rf"
- SQL-Injection
  bypass SQL Commands by User input
  Input: "User=Alice' -&Pass=Idontknow"

advanced techniques
-- IDS evasion --

- bypass IDS by manipulating the patterns
- fragrouter supports all known techniques

  examples:

  Unicode in case of ASCII

  replace www.target.com/etc/passwd with www.target.com/etc/./passwd

  fragmentation of packets on IP Level

thank you

- LinuxDays 2006 from 25.01.2006 - 27.01.2006

- Recommend readings:

- Google Hacking – Syngress - Johnny Long – ISBN 1-931836-36-1
- Physical Device Security – Syngress – Drew Miller – ISBN 1-932266-81-X
- Buffer Overflow Attacks – Syngress – James C. Foster – ISBN 1-932266-67-4
- Staeling the Network – Syngress – Ryan Russel – ISBN 1-931836-87-6
- Stealing the Network – Syngress – 131ah - ISBN 1-93183605-1
- Zero-Day Exploit – Syngress – Rob Shein – ISBN 1-931836-09-4
- Hacking: The Art of Exploitation – APress – Jon Erickson – ISBN 159 327 0070