the hacker's choice

The Future of Hacking

An European View

van Hauser, THC

vh@thc.org

http://www.thc.org

ontents

bout THC

History

- Founded on 1st October 1995 by joining Drunken Traders Inc. and LORE BBS
- First we came up with a cool acronym (THC) and then thought about what it could mean.
- We finally agreed on “The Hacker’s Choice”
- Hey, we were kids back then ☺
- We were and still are a release group. Who wants to join has to release something pretty cool under the THC label.

bout THC

Today

- No one of us is breaking into systems, or committing other computer crimes.
- Wide scope of interest:
  - Network Security/Hacking >> parasite, hydra, flood, probe, gg
  - Unix Security/Hacking >> unix-hacking-toolkit
  - Windows Security/Hacking >> ipf, happybrowser, cupass
  - Application Security/Hacking >> amap, vmap, ra-bbs-hack
  - Credit Card generation/verifying tools >> thc-cred, thc-shagg
  - Wardialing >> thc-scan
  - Wardriving >> wardrive, thc-rut
  - Phreaking >> pbxhack, gd, login hacker
  - Cryptography/Anonymity/Authentication >> passid, fuzzyfingerprints, anon unix
  - Trojans and Backdoors >> ra-bbs, rwwwshell
  - Exploits >> realserv, lpset, thc-sql etc.
  - Ethical articles >> hackers go corporate, human2hacker
  - … and in old times also anarchy and virus stuff … examine our magazines!

bout THC

Our Web Page

- Has got all our tools (29!), articles (32!) and exploits (8) online.

Visit us at http://www.thc.org

The Future Challenges … for a Hacker …

- Operating Systems off the shelf are more secure than years ago
- Source Code Audits done on critical code for all operating systems
- Buffer Overflow Protection techniques will make exploitation harder
- Intrusion Detection Systems alert prior/after intrusion
- Security Knowledge of Admin and Management gets better and better
- Patches are issued faster and implemented faster on systems
- Desktop Firewalls common
- Anti-Virus Software gets better and better detecting trojan horses

What do good Hackers do?

They adapt…

OTE

- During the presentation, some stuff will be highlighted:
  - **blue - means that that this technique will be shown/trained during the Elite Hacking Course at the end of the conference**
  - **green** - means that such software already exists
  - **yellow** - means that such software partially exists
  - **red** - means that such software does not exist – yet …

The Future of … External Reconnaissance

- Strong filtering and better monitoring makes attacking harder
- Until now just rushing at the target – scanning and exploiting – was all it was needed
- In the future, low profile techniques will be used to hide the planning phase of the attacks:
  - Use Web/Internet information extensively
  - Perform elite network topology mapping
  - Identify application of public services (Web, SMTP, DNS)
- No port scans done directly – these are done a month prior attacking from a sacrificial server and only to selected ports and systems
- This way, the attacker knows the target well – the victim can't see it coming

The Future of … Attacking

- The problem: exploits will get a scarce resource
  - Hackers will do more vulnerability research on their own:
    - Source Code Analysis
      - Public and Closed Source (there is more out there than you think!)
    - Binary Code Analysis
    - Monitor Changes to important software (CVS changes to OpenSSH, Apache, Bind, PHP, etc.
  - Hacker won't publish vulnerabilities, but trade with fellow hackers
  - They collect application type and version of their selected targets, and once something is found, exploit these at once
  - As vulnerabilities won't be "*boom* I'm admin" in the future, Hackers will look for smaller vulnerabilities, and use several together as a trampoline to compromise a system

The Future of … Keeping Access

- Once an attacker has access, access has to be maintained
  - Kernel Backdoors
    - Direct Kernel patches will become prominent (vmlinuz, HAL, etc. as well as direct memory tampering of the kernel)
    - Yes, we will see them for Windows XP and 2003 too of course!
    - Loadable Kernel Modules will become obsolete, as they are too easy to detect and defend against
  - System Backdoors
    - Library/DLL manipulation will be performed more often, especially on Windows
  - Backdoors will be *much* better:
    - Hidden - they open up on special events, e.g. packet data (GET to a special web page)
    - Take over the session inline
    - Allow reverse connects to the attacker
    - Take over local user session to further plant backdoors and gain access

The Future of … Preventing Trace Backs

- More systems in between as hops
- Special software to transparently proxy attacks (will be shows on next slide)
- Using Wireless LAN access points of nearby victims to access the Internet
- Backdoors will prevent logging and freeze system if online forensic is attempted

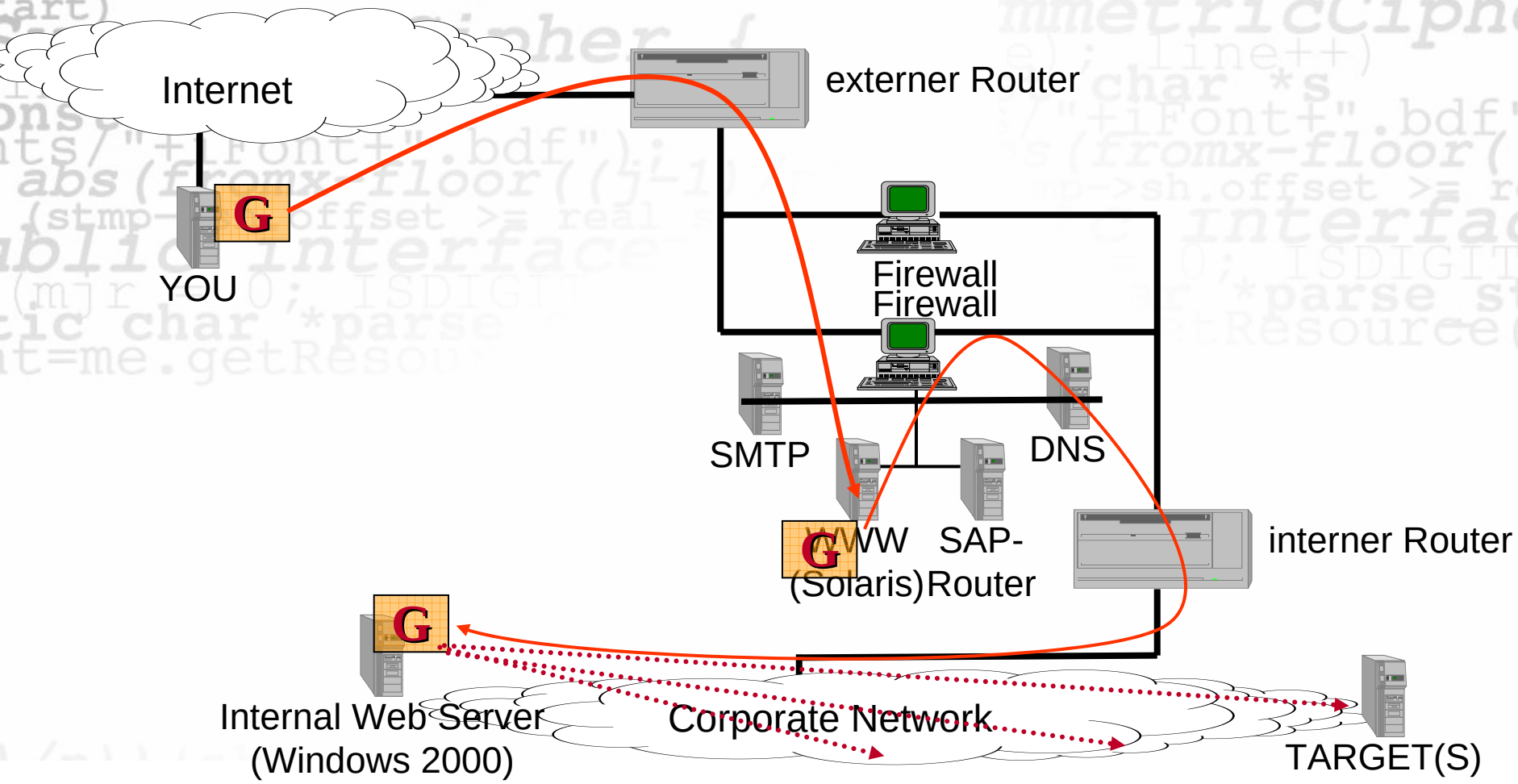
The Future of … Internal Reconnaissance

- Internal Network Intrusion Detection is a problem, therefore:
  - Passive operation system fingerprinting is performed
  - Passive application fingerprinting is performed
  - Passive internal network mapping

The Future of … Internal Attacks

- Internal Network Intrusion Detection is a problem, therefore:
  - Directly attack identified vulnerable applications, no scanning whatsoever!
  - Use encryption and tunneling to defeat the IDS
  - Use transparent proxy software to attack internal systems cross firewalls (this wont also require attack tools to be installed on hop systems)

transparent attack proxy: Grenzgaenger[THC]



looks like this ...

```
laptop:/prg/grenzgaenger-alpha # gg nmap -sT -n -P0 -p 100-113 81.161.148.208

Starting nmap 3.27 ( www.insecure.org/nmap/ ) at 2003-08-08 17:07 CEST
gg-intercept: connection to proxy established
Interesting ports on 81.161.148.208:
(The 13 ports scanned but not shown below are in state: closed)
Port       State       Service
111/tcp    open        sunrpc

Nmap run completed -- 1 IP address (1 host up) scanned in 1.414 seconds
laptop:/prg/grenzgaenger-alpha #
```

looks like this ...

```
laptop:/prg/grenzgaenger-alpha # ssh vh@81.161.148.210
Password:
vh$ cd /tmp
vh$ ./ggd
Info: Admin connect from 81.161.148.222
Info: Admin connection successfully initiated
Info: Connect id 53050 to 81.161.148.208:109/tcp - failed
Info: Connect id 53051 to 81.161.148.208:104/tcp - failed
Info: Connect id 53052 to 81.161.148.208:112/tcp - failed
Info: Connect id 53053 to 81.161.148.208:111/tcp - success
Warning: Request to close connection NOT fulfilled, id 53054 was not found
Info: Executed close command on connect port
Warning: Request to close connection NOT fulfilled, id 0 was not found
Info: Connect id 53055 to 81.161.148.208:113/tcp - failed
Info: Connect id 53056 to 81.161.148.208:102/tcp - failed
Info: Connect id 53057 to 81.161.148.208:106/tcp - failed
Info: Connect id 53058 to 81.161.148.208:105/tcp - failed
Info: Connect id 53059 to 81.161.148.208:108/tcp - failed
Info: Connect id 53060 to 81.161.148.208:107/tcp - failed
Info: Connect id 53061 to 81.161.148.208:103/tcp - failed
Info: Connect id 53062 to 81.161.148.208:100/tcp - failed
Info: Connect id 53063 to 81.161.148.208:101/tcp - failed
Info: Connect id 53064 to 81.161.148.208:110/tcp - failed
vh$ exit
laptop:/prg/grenzgaenger-alpha #
```

The Future of … Worms

- Yes, they will still be there
- They will be more rare
- They will come in more variants
- And yes, we will see some with even faster distribution and damage functions

The Future of … Wireless LAN

- Many, many open
- WEP keys easy to crack (weak password problem)
- Interesting network access
- Well … like it is today ☺
- (we will do some warwalking/wardriving tomorrow in the Elite Hacking Course ☺) [but we stay legal!]

uestions?

Have a lot of fun!